

CYBERQUEST Documentation

English

2026-11-03

Table of Contents

Introduction 7

Get Started 7

Access Web Interface 13

First Steps 13

Licensing 25

Set-up 28

Installation 28

Distributed Architecture 72

Upgrades 81

Data Sources 89

Introduction 89

Tag based Parsing 89

Supported DataSources 92

Data Scanner 95

Operating Systems 98

Networking 102

Applications 105

Databases 117

Threat Intelligence 118

MetaData 119

Vulnerability Scanner 119

Data Deduplication 119

Web Interface 122

Introduction 122

Using Searches 134

Dashboards Module 138

CyberGlance 179

Reports Module 183

Browser 201

Alerts Module 218

Alerts Overview 263

Security Posture 266

Ueba Module 271

Performance Module 279

Executed Schedules 281

Case Management 282

User Actions 300

Threat Intelligence 308

Overview 308

Providers 312
Built in Automatic Alerts 313
Correlation 315
Introduction of Correlation 315
Types of Correlation 315
Managing Correlation Alerts 316
Default Correlation Alerts 318
Vulnerabilities 365
Overview 365
Vulnerability Reports 375
Vulnerabilities Dashboards in CYBERQUEST 380
Settings 384
Application Settings 384
Alerts 422
Data flow rules and filters 425
User and Group Management 432
Data Scanner 439
Management 446
Jobs 487
Tools 491
Marketplace Importing and Exporting Extensions 495
CYBERQUEST API 501
Collectors 501
Communications 508
DataSources 512
Internals 512
Parsers 513
Utilities 515
Actions 518
Integrations 520
Automatic Lookback on Events 524
Support 527
Frequently Asked Questions 527
Additional utilities 534
Troubleshooting 535
Maintenance 547
Product Support Lifecycle 551
Editions 554
On prem 554
CYBERQUEST Licensing and Versioning 556
CYBERQUEST in Practice 561
Operational 561

Alerts create logon config 568
Back-up CQ 571
Disaster Recovery 573
CQ EventIDs 579
How-to · AD information needed to read AD objects 581
How-to · Collecting Mysql-data 582
How-to · How to collect in a table from a PostgreSQL database 583
How-to · How to collect logs from AWS CloudFront 583
How-to · How to collect logs from AWS CloudTrail 583
How-to · How to collect logs from Squid 584
How-to · How to configure Apache to send logs to CYBERQUEST server 584
How-to · How to configure CYBERQUEST to collect MS exchange tracking logs 585
How-to · How to configure DarkTrace to send logs to CYBERQUEST server 585
How-to · How to configure File Integrity Monitoring (FIM) on Linux servers 587
How-to · How to configure Firewall CheckPoint to send logs to CQ Server IP Address on port 5140 UDP 590
How-to · How to configure FortiGate to send logs to CQ Server IP Address on port 5140 UDP 595
How-to · How to configure GravityZone to send logs to CQ Server IP Address on port 5140 UDP 596
How-to · How to configure IPS FireEye to send logs to CQ Server IP Address on port 5140 UDP 597
How-to · How to configure Linux server to read custom log files with rsyslog 597
How-to · How to configure Linux server to send logs to CQ Server IP Address on port 5140 UDP 598
How-to · How to configure NetGear AP to send logs to CQ Server IP Address on port 5140 UDP 598
How-to · How to configure NGNIX to send logs to CQ Server 601
How-to · How to configure ODBC client to collect from Oracle DB instances 601
How-to · How to configure Office365 to send logs to CQ Server 605
How-to · How to configure VmWare VCSA 6.7 to send logs to CQ Server IP Address on port 5140 UDP 612
How-to · How to configure WSO2 to send logs to CYBERQUEST server IP Address on port 5140 UDP 613
How-to · How to enable MariaDB auditing 614
How-to · How to enable or disable MS SQL Audit for MSSQL instance 615
How-to · How to enable PostgreSQL auditing 618
How-to · How to enable Print Service audit 620
How-to · How to enable the Audit service for Linux 624
How-to · How to integrate HR system in CYBERQUEST 625
How-to · How to setup Windows Print Logs 625
How-to · How to Setup Windows Sysmon 626
How-to · How to track changes made in Active Directory 627
How-to · OSSEC Configuration 635
Operations · How to activate automatic Actions in Realtime Alerts 636
Operations · How to Add a New Asset 650
Operations · How to avoid split brain in MariaDB galera replication 656
Operations · How to Change CYBERQUEST Administrative Passwords 657
Operations · How to change password web application superadmin password 658
Operations · How to collect data from Check Point Firewall 662
Operations · How to collect data from the Office 365 application 663

Operations · How to collect data on Active Directory Assets Information 665
Operations · How to collect data on Active Directory 667
Operations · How to collect data on Windows Application Log 669
Operations · How to collect data on Windows Security Log 671
Operations · How to collect data on Windows System Log 673
Operations · How to collect IIS Logs with CYBERQUEST 675
Operations · How to connect to Active Directory 680
Operations · How to connect to CQ Threat Intelligence 682
Operations · How to create a Copy job 684
Operations · How to create a DTS Alert 686
Operations · How to create a MariaDB cluster for CYBERQUEST operation 688
Operations · How to create new alerts 696
Operations · How to create a new report and how to run 698
Operations · How to create a parser 701
Operations · How to create a RTBF job 704
Operations · How to create an on-demand dashboard 708
Operations · How to create Backups 710
Operations · How to delete data from Data Storage 715
Operations · How to delete events older than 6 months 718
Operations · How to disable two-factor authentication (2FA) for a user account 721
Operations · How to enable two-factor authentication (2FA) for a user account 723
Operations · How to export data from dashgroup 725
Operations · How to export data from Reports page 728
Operations · How to forward alerts to another host 730
Operations · How to forward syslog data 732
Operations · How to create a new dashboard, dashgroup and view data 734
Operations · How to manage collect CSV Files 738
Operations · How to collect Oracle audit logs 741
Operations · How to manage credentials 744
Operations · How to manage CYBERQUEST data 745
Operations · How to manage Ueba 746
Operations · How to manually deploy agent and assign data sources 755
Operations · How to manually deploy agent for Windows based collections 760
Operations · How to monitor administrative privileges use 763
Operations · How to monitor cyberquest user activities 764
Operations · How to monitor inactive accounts 766
Operations · How to reconfigure WMI settings for remote collect 769
Operations · How to reconfigure WMI Settings Permissions for remote collect 772
Operations · How to restore data from archive 776
Operations · Website certificate import and Email certificate import 779
Operations · Minimum WMI permissions for Domain User Account 787
Operations · Minimum WMI Permissions for Local User Account 793
Operations · Password encoding 797

Operations · VMI Permissions 798
Operations · VMI Ports 802
Third-Party Components 804
Licensing 804
Additional reading 812
Smart Objects 818
CQ Smart Objects 818
Automation 824
Introduction 824
Extending Actions 827
Supported Vendors 829
Troubleshooting 854
Automated Actions 855
CYBERQUEST OS 1565
OS Installation 1565
OS Upgrade 1588
Application Configuration 1589
Development Roadmap 1593
CYBERQUEST Roadmap 1593

Introduction

Get Started

CYBERQUEST Overview

CYBERQUEST is an innovative Big Data Security Analytics Platform designed to provide comprehensive auditing and security capabilities for small, medium and enterprise networks. The solution has been designed to function as an agile, scalable business platform that intelligently collects and correlates data in the organization's IT infrastructure and works with it to address any type of present or future threat which a busine0ss could encounter.

CYBERQUEST is highly scalable and can be configured to suit many organization size and use cases and easily integrates with all security solutions on the market, irrespective of their classification. The CYBERQUEST solution is a true aggregator of security data coming from either Security Information and Event Management software (SIEM), firewalls, intrusion prevention and detection platforms, or email security and endpoint security solutions. In addition, CYBERQUEST can collect, correlate, and provide useful insights on heterogeneous data generated by network equipment, servers, databases, and applications, which makes it an invaluable operational management tool for your security and administrative teams.

Core Capabilities

- Collect: gather all security and relevant data sources from your IT infrastructure;
- Correlate: add threat intelligence security data for offline or online correlation;
- Detect: quickly identify the most significant threats to your network;
- Visualize: monitor accurately within a single point of access and get specific alerts;
- Respond: Security Orchestration, Automation, and Response (SOAR features) capabilities are embedded in the solution;
- Vulnerability assessment: with OpenVAS integration.

CYBERQUEST aggregates and monitors all activity in your infrastructure and, with real-time alerts, SOAR features, and vulnerability assessment capabilities, delivers detailed information and fires response for vital changes and activities - as they occur. Instantly know who, what, when, where, why made a change, and then turn that information into intelligent, in-depth forensics, enhanced with additional data from the entire environment, make that information available for auditors and security officers and generate automated actions as response to the risks associated with day-to-day modifications.

Concept and availability

CYBERQUEST can seamlessly be integrated within your existing IT infrastructure and delivers real-time user behavior and data monitoring, threat detection, data analytics and correlations, security information and event management, in a single platform, enabling you to:

- Have unified and increased infrastructure visibility for security management;
- Ensure and track regulatory compliance, security audits and policy;
- Reduce organization threat surface quickly and accurately;
- Optimize and generate predefined, ready-to-go reports;
- Improve your existing security and event management solution's response capabilities to incidents.

CYBERQUEST is an appliance type of product (hardware & software) supporting multi-redundant topologies and that can be scaled horizontally by installing any number of processing nodes, or vertically by adding processing resources. Given its deployment flexibility, the solution can be easily architected to meet multi-site deployment challenges. The solution is also available through Software-as-a-Service offering.

Its main functionalities, given by multiple modules, are:

- Normalizing available information from different systems in its own format through special dedicated connectors;
- Dashboards module: provides a visual representation of events, aggregated by different criteria;
- Browser module: provides access to all events and viewing the details;
- Reporting module: predefined reports for - GDPR, ISO 27001, COBIT, FISMA, HIPPA, PCI/DSS, SOX, technology reports;
- Alerting module: provides real time alerting for configurable situations with configurable response actions (SOAR features);
- Investigation module: a visual way of seeking events and investigating situations;
- Case management module: a case management function for collaborative investigation activities;
- Administrative module: ensures configuration and management functions for the application;
- Data Transformation System module: a proprietary module that is responsible with different functionalities of CYBERQUEST such as event enrichment, data anonymization etc.
- Vulnerability Assessment Module: provided by integration of OpenVAS (https://www.openvas.org/ (https://www.openvas.org/))

Architecture

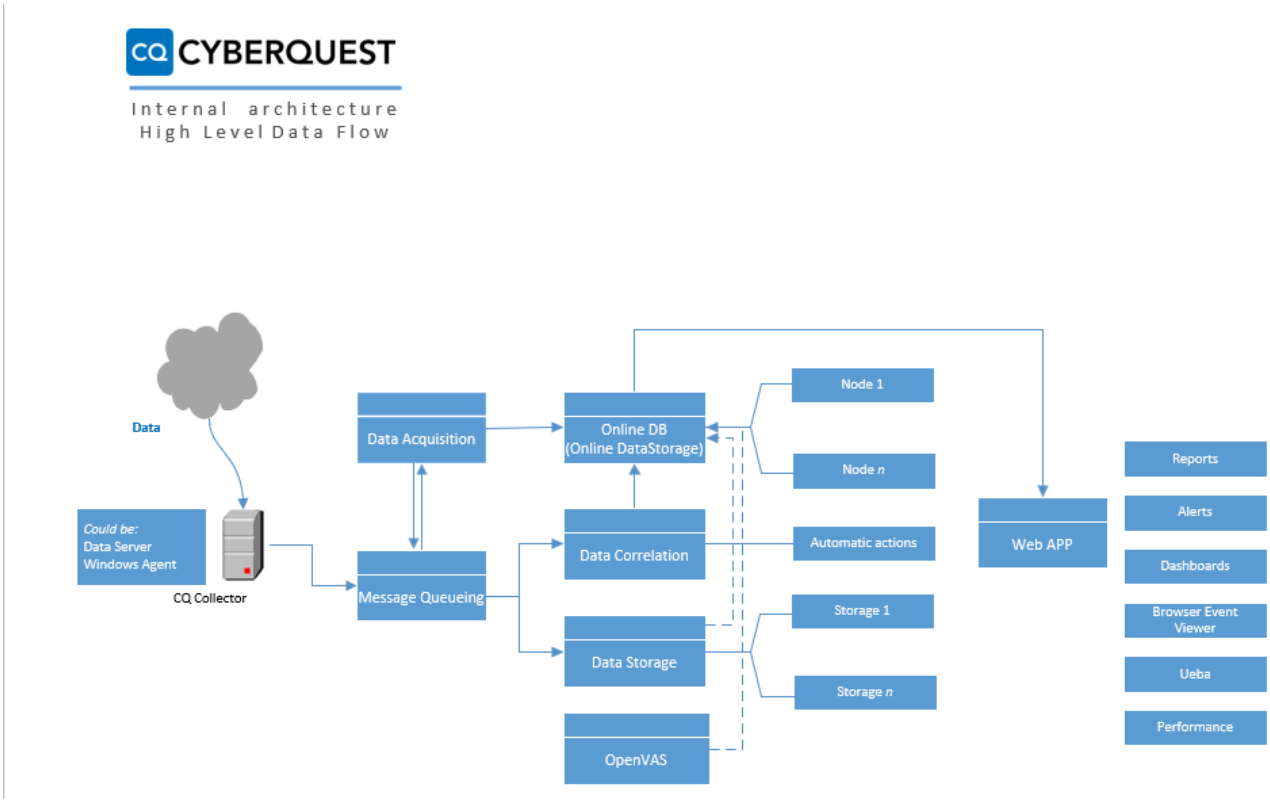
High-level data flow description

CYBERQUEST is a dedicated Big Data Security Analytics Platform intended to be used by IT security officers. Therefore, CYBERQUEST helps companies to be more secure and also compliant to internal and industry regulations by doing collection of high volumes of disparate data from infrastructure and third-party security solutions, aggregating and enhancing collected data, and presenting security personnel with useful information on possible threats and risks - all in real-time.

Data is collected from various sources using CYBERQUEST's Collecting Agent (WMI, ODBC or file-level gathering etc.), or receiving data flows (syslog, NetFlow etc.). Data is organized in queues, sent to a Data Acquisition Service (DAS), which applies acquisition rules and then sends raw data to a Data Transformation Service (DTS). DTS is responsible for parsing data and generate real-time alerts.

Once parsing rules are applied, transformed data is applied with retention rules. Retention rules will tell if data is stored in the Online Storage or Archive Data Storage. The major difference between the two types of storage is access speed. Online Storage applies indexing on uncompressed data, which makes any information available in term of seconds, with the cost of space. Archive DataStorage is designed for long term retention of data, without imposing a limit to the maximum volume of that data. The archive stores data in compressed and encrypted files; the norm compression ratio is approximately 1:20.

CYBERQUEST supports log storage using both local HDDs and NFS (Network File System). Local HDDs can be used for operational and archive storage, while NFS enables the Archive Data Storage to use centralized storage resources provided by the beneficiary.



From the archive data is extracted and imported into Online DataStorage nodes for investigation and reporting needs. Correlation is performed by a CYBERQUEST Server and resulted information is presented in dashboards and reports.

CYBERQUEST Web Interface is the central module used for both management and utilization of platform. Web Interface uses a web frontend allowing administrators and operators to interact with CYBERQUEST. Depending on the access level allowed, a user will be able to access Reports, Dashboards, Investigations, Browser and Alerts modules and take benefit of the entire set of security analytics.

Services and Components

Data Collection

CYBERQUEST receives data from a wide range of devices. The data collected is of various formats, but mainly separated into sections as it follows: collection of event data, flow data, vulnerability assesment information (VAI), and other data types relevant for security analytics.

Event data collection: events are being collected from data sources that log security-based events, such as: routers, servers, firewalls, intrusion detection systems (IDS) or intrusion prevention systems (IPS), network switches, active directory and other networking equipments.

Flow data collection: network traffic information is collected from IPFIX and Netflow network protocol (versions 5, 9, and 10).

Vulnerability assessment (VAI): relevant security states.

Data Collection is a distributed service, engaged with several components that can reside within the main appliance, or independently to accommodate star or cloud architectures. Once collected, data is encrypted and compressed, then transported by the message queuing sevice to the data aquisition service.

If data cannot be delivered to message queuing service, one of the following agents will perform local caching for later delivery:

- Windows Agent, capable of storing up to 1 million events.
- Data Server performs caching behaviour when needed, by creating files on the hosting station in order to capture all events, without any event being lost during the process.

Windows Agent

Windows Agent is a data collection component, interacting directly with event sources. It can be installed on workstations and servers. The minimum operating system version is Windows 7 (on workstations) and Windows Server 2008 (on servers), and has a listed software dependency on Microsoft .NET Framework 4.8.

- Windows agents installed on versions older than **Windows 11 or Windows Server 2022** need to be updated within the **Docker** environment. On terminal CYBERQUEST machine , navigate to `cyberquest-deployment` folder and edit the `.env` file by running the following command:

```
nano .env
```

Add the following line to the file:

```
SSL_PROTOCOLS=TLSv1.2 TLSv1.3
```

- Windows agents installed on versions older than Windows 11 or Windows Server 2022 need to be updated within the **dpkg environment**. On terminal CYBERQUEST machine edit the custom file by running the following command:

```
sudo nano /etc/nginx/sites-enabled/custom
```

Edit the following line to the file:

```
ssl_protocols TLSv1.3;
```

The agent uses configuration templates that can be associated to one or multiple data sources. The templates contain settings specific to data sources: credentials, field mapping, event filtering, data processing scripts, database queries and more.

The agent addresses the following data sources by default:

- Local and remote WMI (Windows Management Instrumentation) collection:
  - Windows Security logs;
  - Windows Application logs;
  - Windows System logs;
  - Other application and services logs in Windows standard format.
- Local and remote MS SQL collection:
  - Queries for incremental data collection from database tables; containing application logs (minimum version supported is MSSQL Server 2005);
  - SQL Server audit (minimum version supported is MS SQL Server 2008) by default.
- Local and/or remote Oracle collection:
  - Queries for incremental data collection from database tables containing application logs (minimum version supported is Oracle 9i);
  - Native Oracle instance audit; by default, the solution provides templates for Oracle 9i, 10g, 11g and 12c.
- Custom data collection (which requires parameters and mappings to be configured in each customized template):
  - Local and/or remote collection for ODBC (open database connectivity) sources supporting 64-bit ODBC drivers;

- Local and/or remote collection for MySQL, MariaDB, PostgresSQL, MS-SQL sources, including queries for incremental data collection from database tables containing application logs and native platform audit;
- Local collection of timestamped files in CSV/TSV/JSON format;
- Local collection of parsable custom files of any file type, for which the agent uses a pre-processing script;
- HTTPS API-based data;
- Others.

Data Server

Data server is a distributed service engaged with several components that can reside within the main appliance, or independently to accommodate star or cloud architectures. The service is used to perform data pre-parsing on syslog native format compatible with RFC 5424 and RFC 3164 standards. The system can also receive and process NetFlow data (NetFlow versions 5, 9, 10 and ipfix) and perform NetFlow stiching called Biflow.

Also, Data Server acts as a passive agent for syslog and NetFlow messages received by CYBERQUEST. By default, the service is configured to listen on UDP/TCP 5140 port for syslog events, UDP 2055 for NetFlow packets, TCP 5141 for CEF data, TCP 6514 For Syslog on TLS protocol.

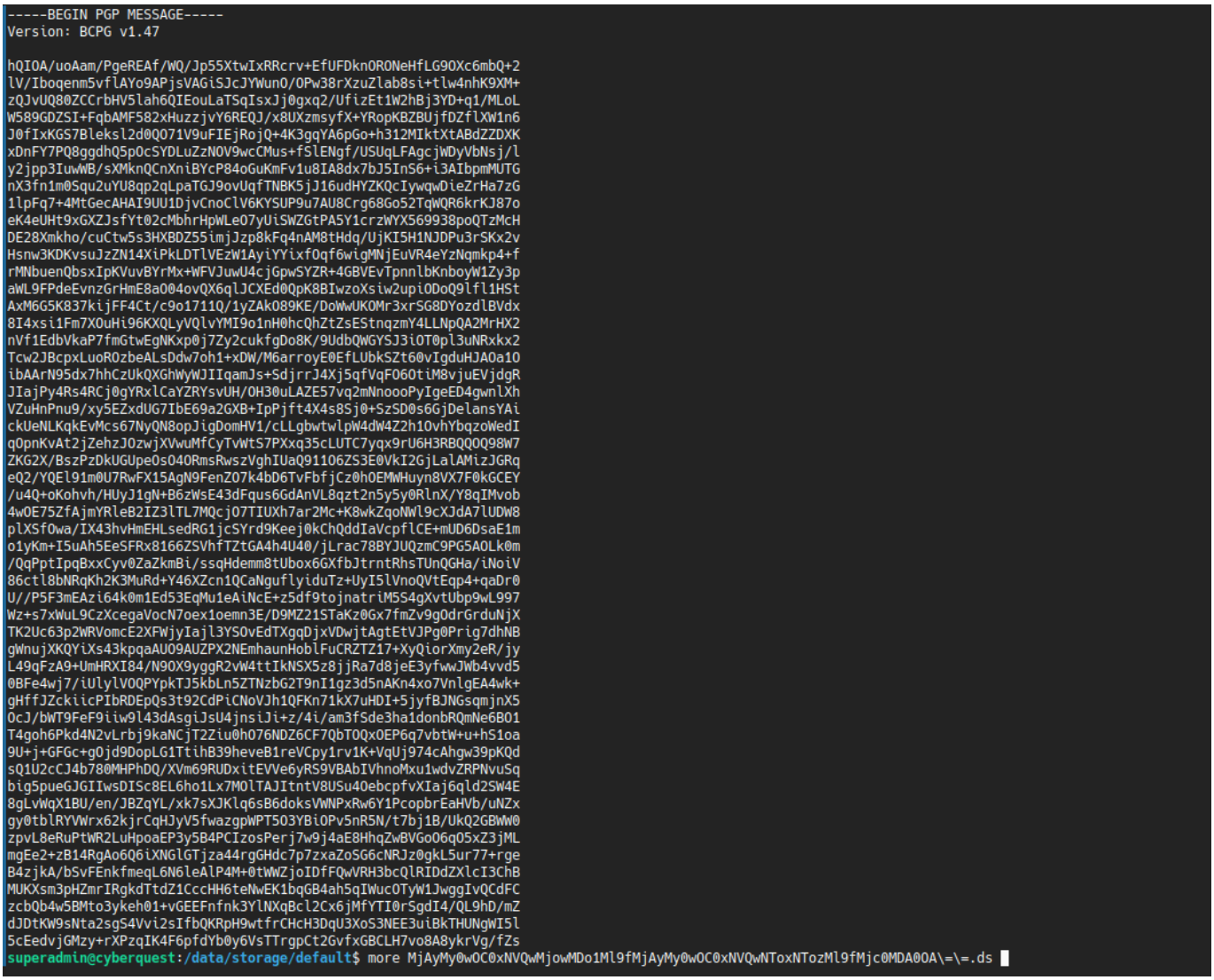
Data-Server and Windows agent employ secured communication to the central CyberQuest server using 2 types of complementary encryption:

1. Native SSL encrypted connection to RabbitMQ on the server on port 5671 (default).
2. Additional AES-256 encryption for all messages (logs). This can be enabled by using the “Encrypt” parameter at agent level.

Data Storage

CyberQuest stores date in 2 parallel places: OpenSearch for immediate investigations, and the Data-Storage service. Data kept in the data-storage service is file system based, includes automatic compression, encryption and employs for data alteration reasons digital signature protection.

The default installation includes a “default” storage under “/data/storage/default”. All incoming data is automatically sent to this storage. DataStorage employs a special file which hosts event data: “.ds” file. This file is pgp signed so that any alteration will not validate the signature anymore.



Encryption keys are automatically generated and MUST have backups. NextGen Software CANNOT recover the data if these are lost. These are stored under:

```
ls /var/opt/cyberquest/encryption/datastorage
```

Access Web Interface

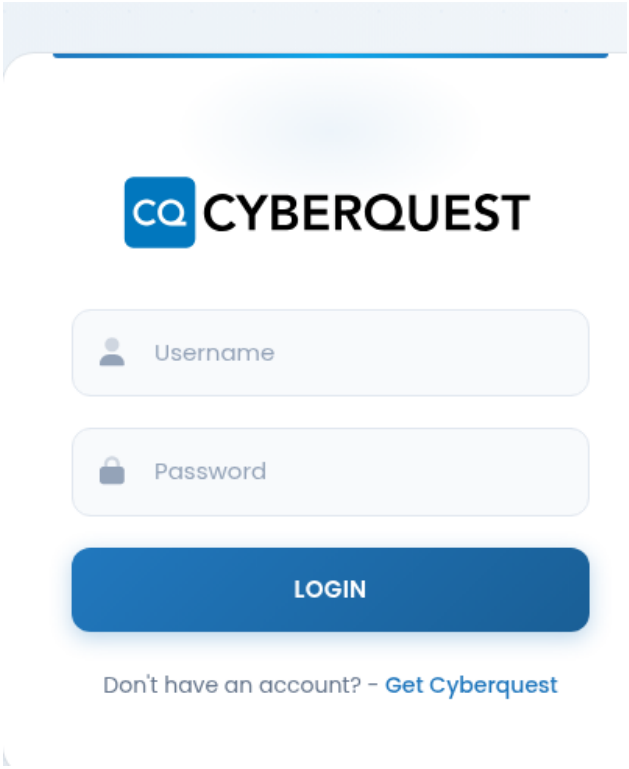
First Steps

Accessing the web interface

Web Interface is a consolidated web frontend hosting all administration and operation functionalities of CYBERQUEST. The web interface is compatible with all major browsers on the market.

To access Web Interface, open a web browser and type the application's address or DNS name. The default address initially assigned to Web Interface is ***https://CyberquestIPAddress*** (example).

The browser automatically redirects you to CYBERQUEST's authentication page:

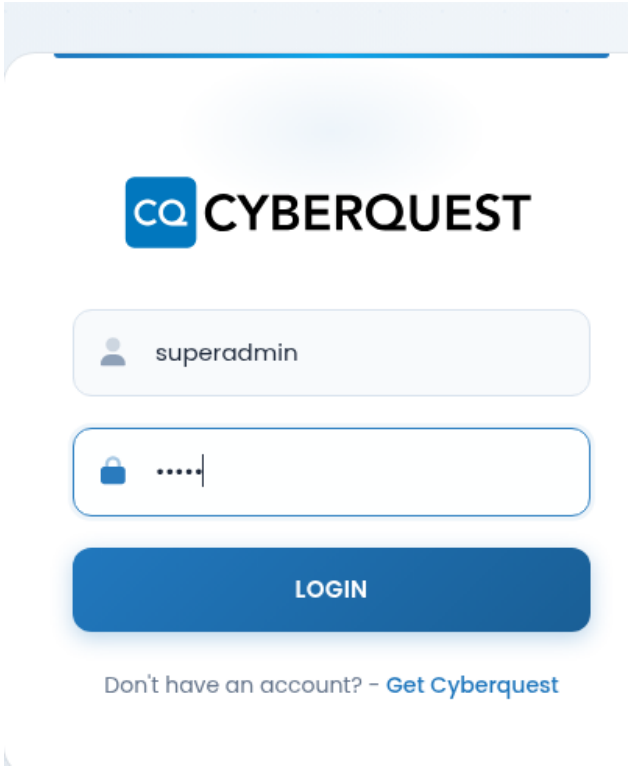


User Authentication

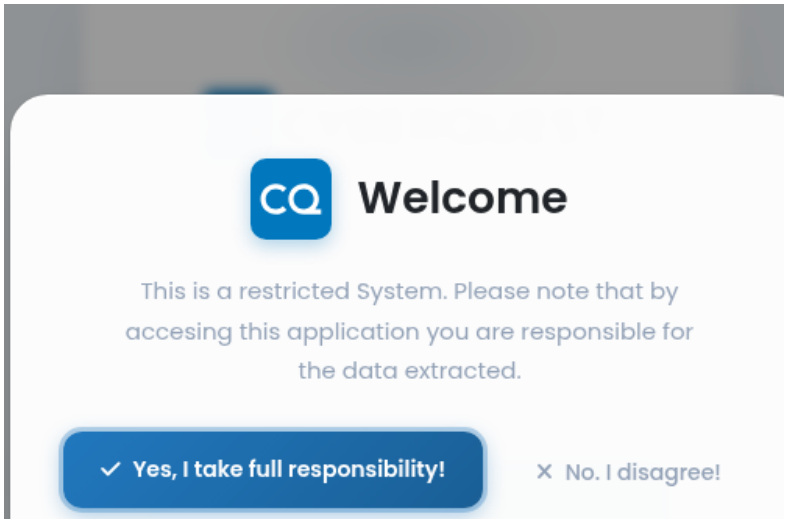
Authentication can be accomplished in one of two ways:

- Using a local user defined in the application;
- Using a company's Active Directory user. This facility allows authentication with Active Directory credentials when LDAP integration has been configured within application. The user must belong to one of two Active Directory security groups: "CYBERQUEST Administrators" or "CYBERQUEST Users".

  Type the default username and password, then select the interface language.



You will be prompted with a default message about accessing restricted information. This message is fully customizable.



Accept the responsibility by clicking the button ***Yes, I take full responsability!***. Else ***No. I disagree!*** and you will be redirected to the authentication page.

The initial authentication is performed under the default administrative account. When authenticating as administrator, an additional confirmation box is displayed. This additional authentication step was introduced to notify on indiscriminatory access to the entire platform configuration and to require user confirmation of acknowledgement. Superadmin activity should be performed with maximum responsibility and knowledge of platform's administration. Wrongfully changing configuration, rules and retention policies can break access to analytics data, delete or damage objects, and more important, can cause permanently loss of history data.

Changing User Password

Once authenticated, a user can change his password from User menu. This is a strongly recommended action after the first login, and it can be performed at any time forward. In order to change your password, access **User > Change password** option.

To see how to change the password, please follow the link: Changing user password

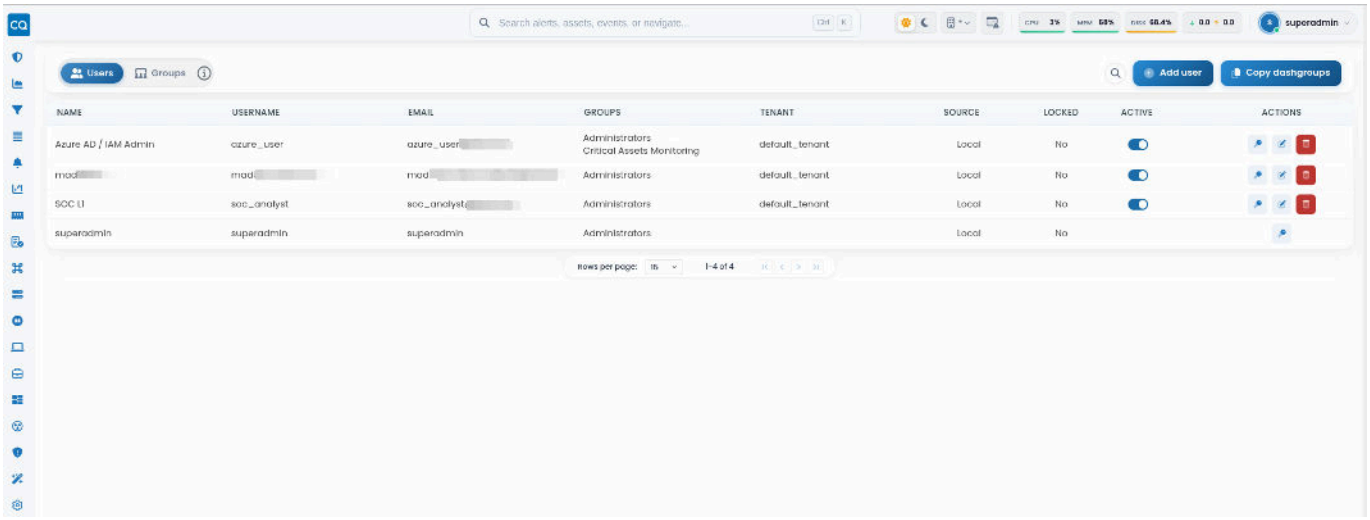
Managing Users and Groups

Role Based Access Control (RBAC)

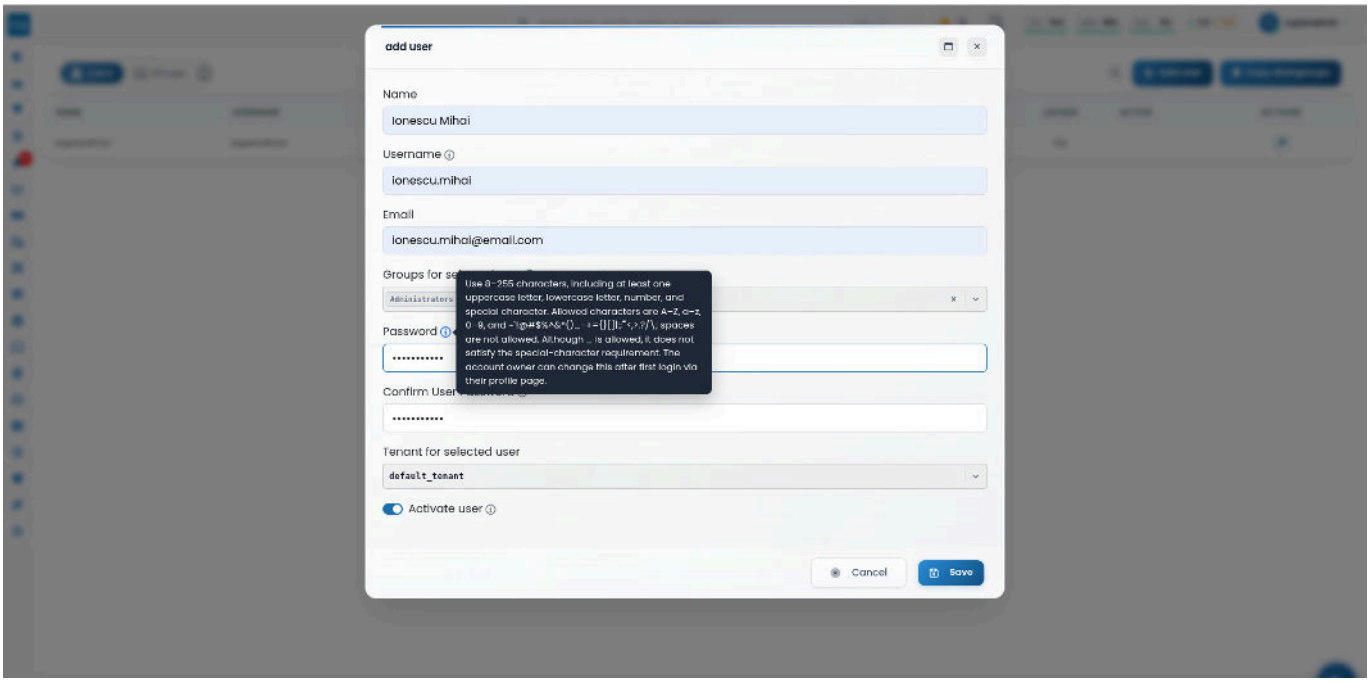
User accounts created can be configured to access components based on the user role assigned to their account. You can add or edit user roles and user accounts as needed.

Add a new user

- Log in to CYBERQUEST with an administrative account.
- Navigate to **Settings > Users and Groups > Users**.



- Click **Add user**.



Configure the user account by specifying:

Name - Specifies the full or display name of the user account.

Username - Defines the unique username used by the user to authenticate in CYBERQUEST.

Email - Specifies the email address associated with the user account.

Groups for selected user - Assigns the user to one or more groups, inheriting the roles and data-access permissions configured for those groups.

Password - Defines the password used by the local user account for authentication. The password must contain **8–255 characters** and include at least **one uppercase letter, one lowercase letter, one number, and one special character**; spaces are not allowed.

Confirm User Password - Confirms the password entered for the user account and ensures both password values match.

Tenant for selected user - Associates the user account with the selected tenant and determines the organizational scope in which the account operates.

Activate user - Enables or disables the user account and controls whether the user can access CYBERQUEST.

- Click **Save** to create the user.

Add or edit User Roles

User roles are assigned to user accounts to control access in Web Interface. You can add or edit user roles as needed. Roles are assigned at group level.

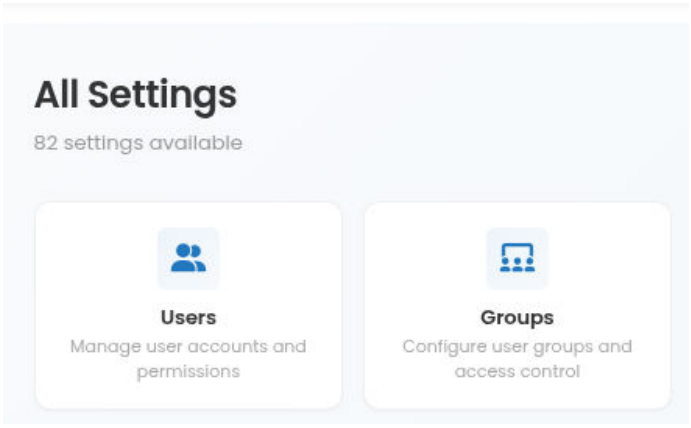
In order to add or edit user roles:

a. Login to application with an administrative account.

b. Navigate to Settings menu by pressing



button, in the left side of the interface where are the quick access buttons, then click *Groups.*



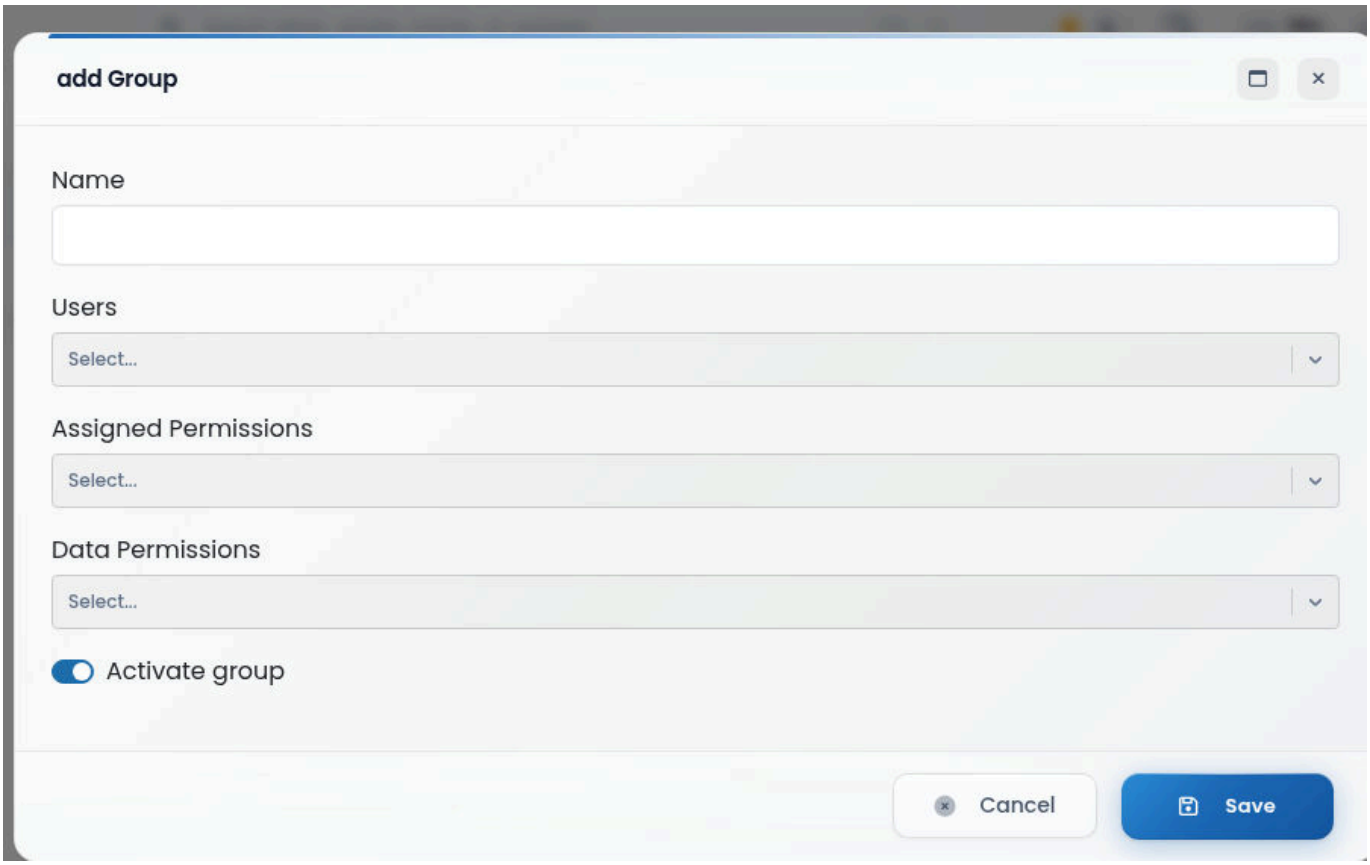
c. **Groups** configuration page opens:



d. In **Groups** page, click



button and the window will open:



In the **Name** field, you have to provide a name, such as Users Restricted Permissions.

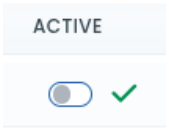
In the **Users** field, select the users that will be impacted by the predefined rules.

In the **Assigned Permissions** field, select the appropriate permissions for the selected users.

Decrypt permission - Users who are members of a group with the **Decrypt** permission can view the original values of anonymized fields. Users who do not belong to a group with the **Decrypt** permission will see the anonymized values when accessing event data in CYBERQUEST components such as Browser and Reports.

In the **Data Permissions** field, you have to select the appropiate data and the selected users can view.

e. By default the new group is enabled. Deactivate the group by selecting



option.

f. Press “Save” button to add new defined group and close the window or press “Cancel” button to close the window without saving changes. As an option, you can close the window without saving changes by clicking the

mark in top-right corner.

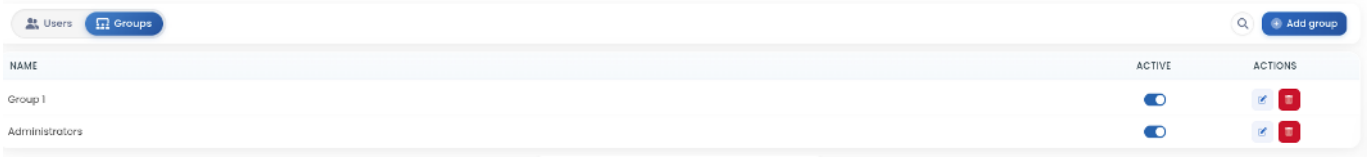
Delete User Groups

To delete a group, navigate to Settings menu by pressing



button, in the left side of the interface where are the quick access buttons, then click **Users and groups > Groups** . Press

icon and confirm deletion of desired group. The procedure is irreversible. Built-in groups cannot be deleted.

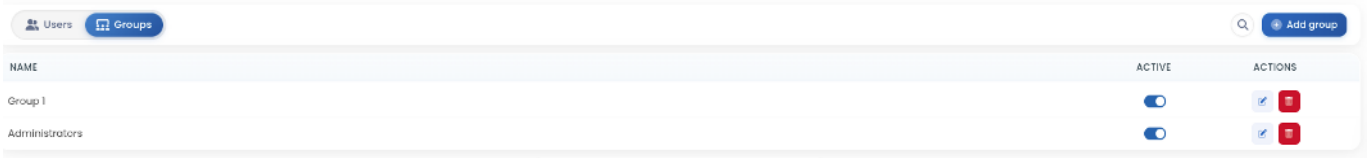


Edit User Groups

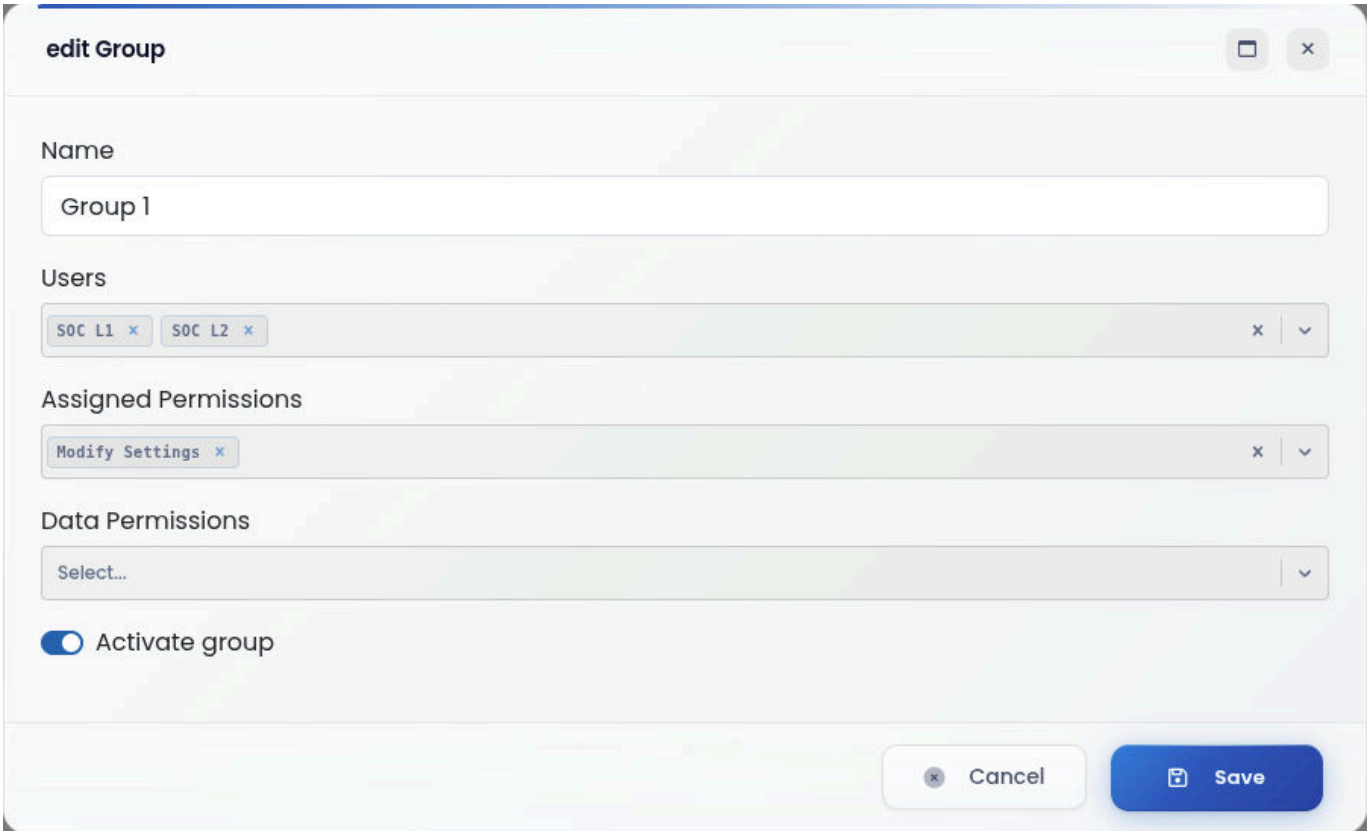
To edit a group, navigate to Settings menu by pressing

button, in the left side of the interface where are the quick access buttons, then click **Users and groups > Groups**. Press

icon and the edit group window is displayed where you can change group name, group members, assigned permissions and data permissions.



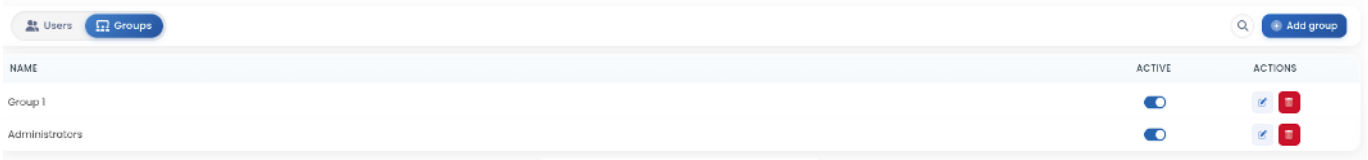
Changing group members, assigned permissions and data permissions is one by selecting or de-selecting objects in each drop-down list.



Press “Save” button to save changes and close the window or press “Cancel” button to close the window without saving changes. As an option, you can close the window without saving changes by clicking the

mark in top-right corner.

You can also change group status being **Enabled** or **Disabled**. Group status can be quickly changed from main Groups window by actioning on **Active** option button and selecting **On** or **Off**. In this case, changes are saved automatically.



For built-in groups you will only be allowed to add or remove members.

Dashboards migration

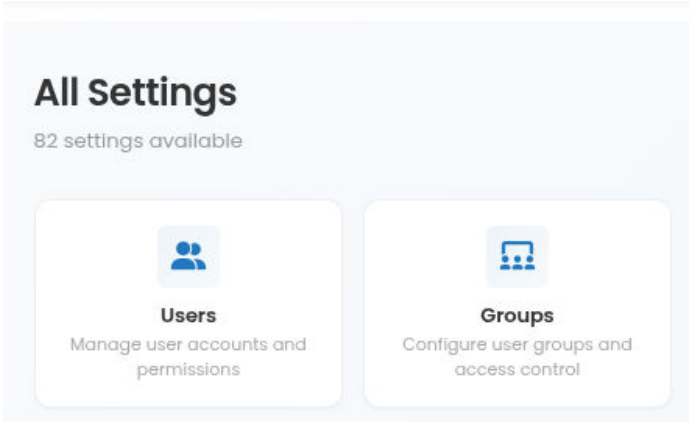
Each user can create his own dashgroups containing its own dashboards, but only an administrator can migrate a dashboard from a user to another. After creating a new user, an administrator can copy dashgroups from another user that already has dashgroups configured. To do this, follow the next steps:

a. Login to application with an administrative account.

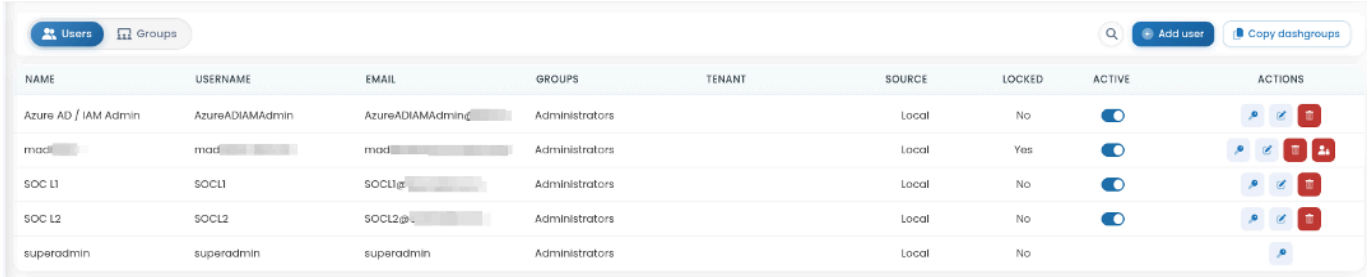
b. Navigate to Settings menu by pressing



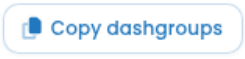
button, in the left side of the interface where are the quick access buttons, then click **Users and groups > Users**.



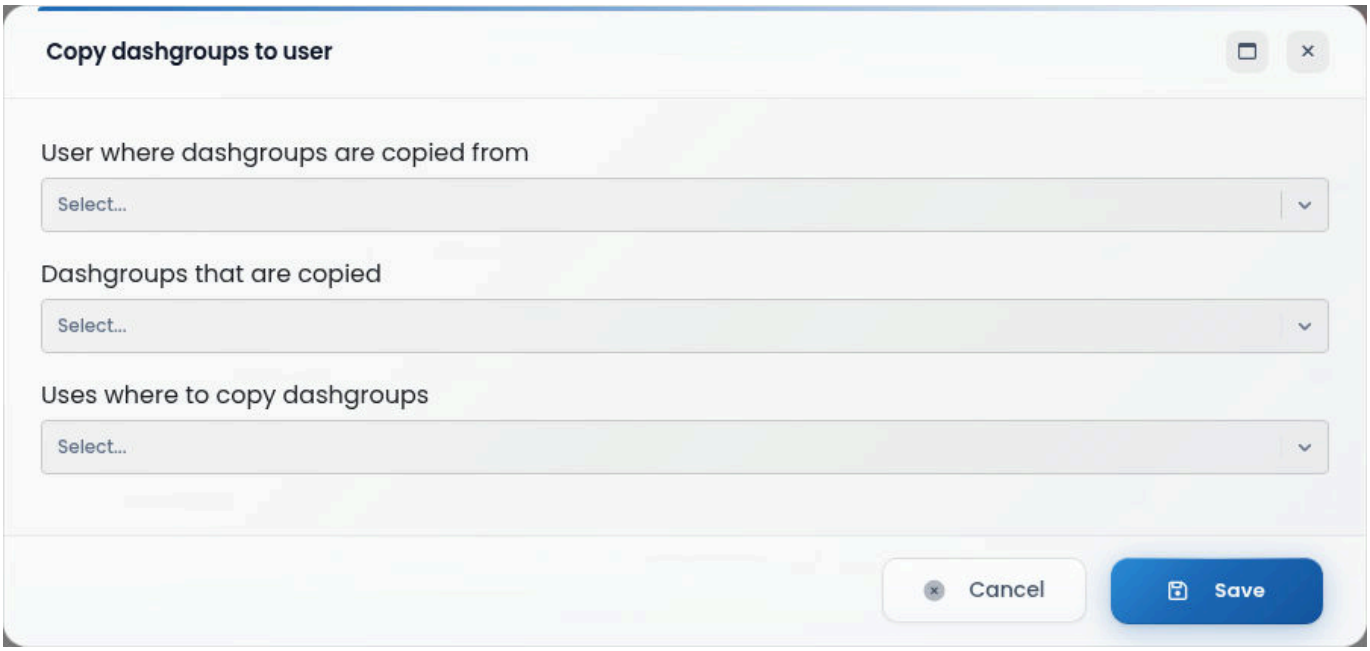
c. **Users** configuration page opens:



d. In Users page, click



button and window will open:



Check source and destination users from **User where dashgroups are copied from** and **Users where to copy dashgroups** drop-down lists. Select desired dashgroups from **Dashgroups that are copied** drop-down list and press "Save" button to save changes.

e. Logout from the administrative account and login with the new user account. After login is successful, the Dashboards module will show the new dashgroups selected during previous step.

Data permissions

CYBERQUEST provides data permissions options, which combined with the role-based access features offers a granulized control over the data made available for user members of a group. Data permissions are set at group level.

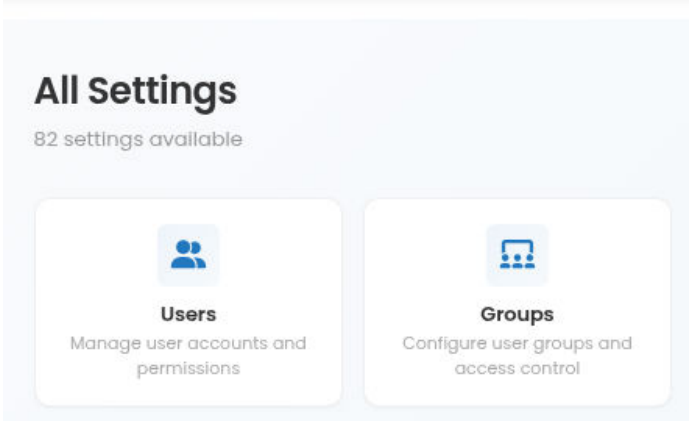
In order to change data permissions for an existing group, follow these steps:

a. Login to web interface with a user with administrative rights.

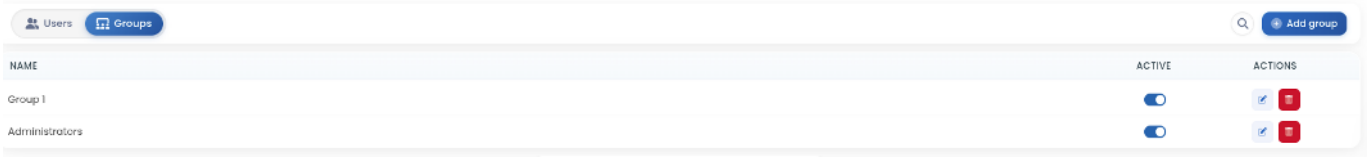
b. Navigate to **Settings** menu by pressing



button, in the left side of the interface where are the quick access buttons, then click **Users and groups > Groups**.



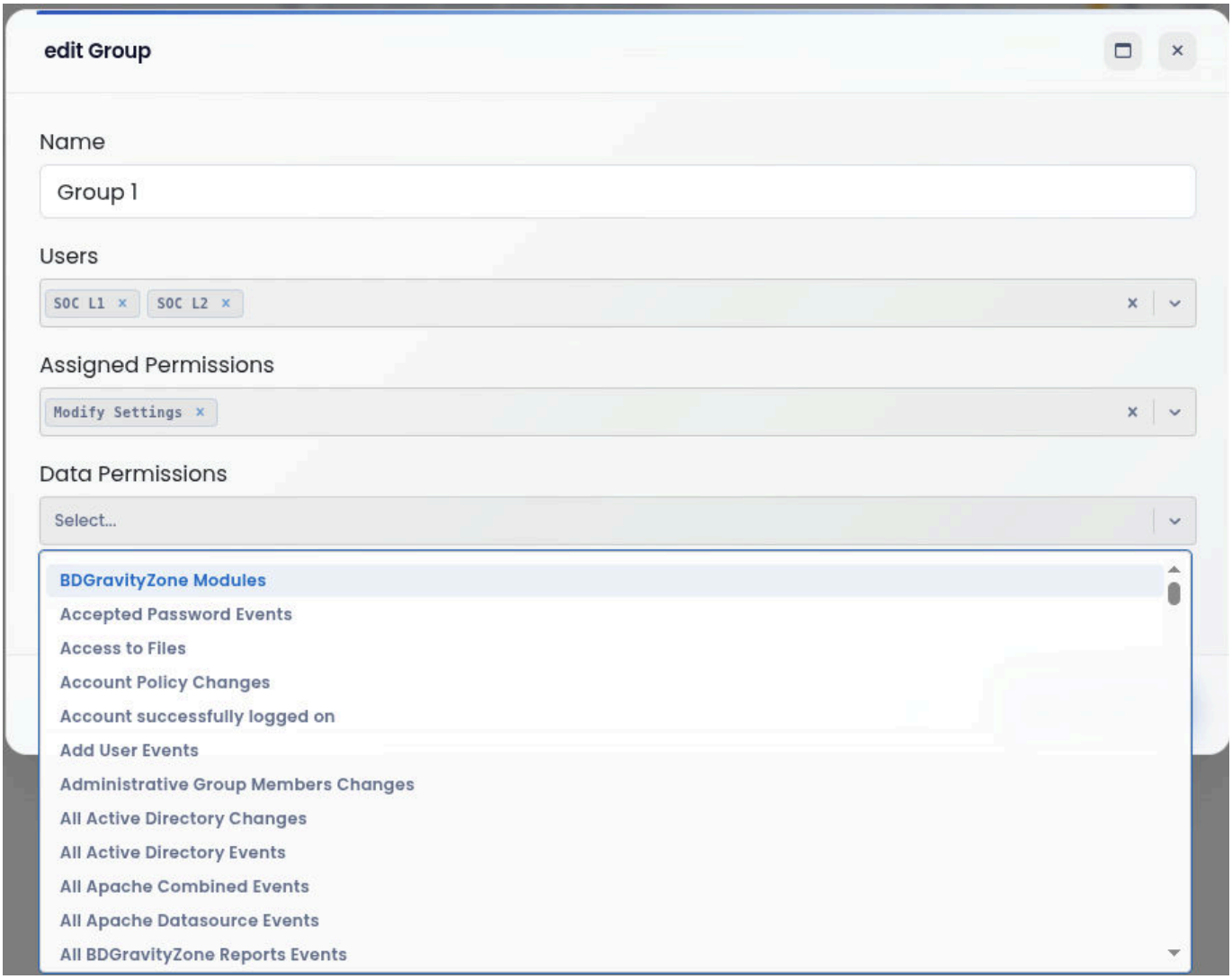
c. **Groups** configuration page opens:



d. In **Groups** page, you have to press



button, for the group containing the user for which you want to change data permissions. **Edit group** window opens.



In **Data Permissions** field select or deselect on the appropriate data permissions. If no filter is selected, the user will have unrestricted access to all data available.

e. Press “Save” button to save changes and close the window or press “Cancel” button to close the window without saving changes. As an option, you can close the window without saving changes by clicking the

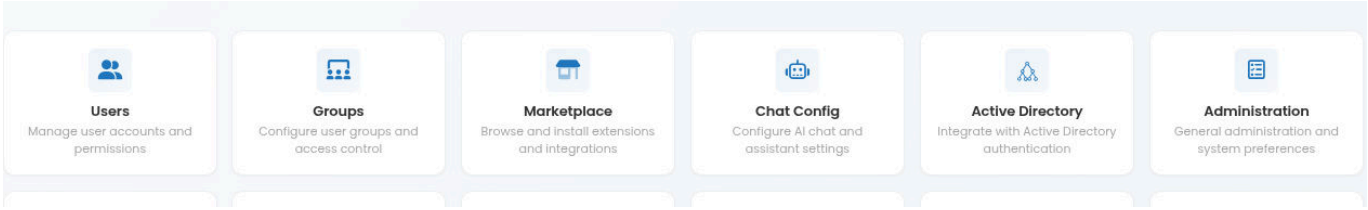
mark in top-right corner.

Configure LDAP authentication

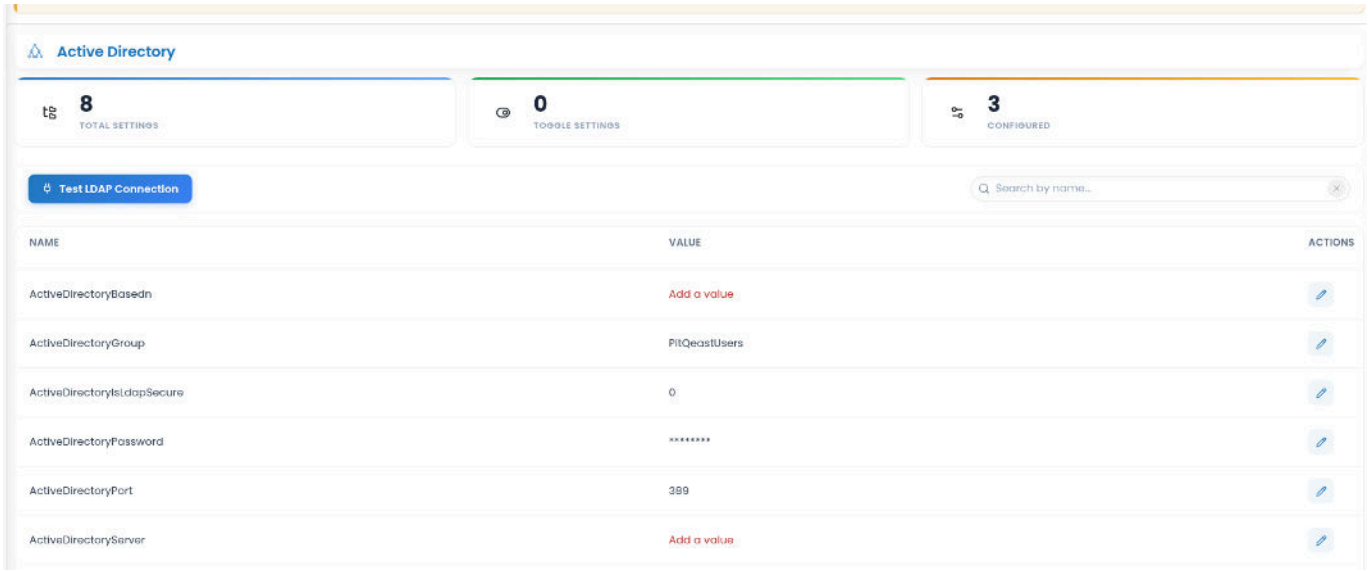
CYBERQUEST can be integrated with Active Directory or LDAP systems, allowing users to directly authenticate to CYBERQUEST. To do this, please follow these steps:

a. Login to web interface with a user with administrative rights.

b. In web interface select **Settings > Application Settings > Active Directory**.



c. **Active Directory** configuration page opens.



The following fields can be edited:

- **Active Directory Basedn**: Location of the user used to connect to Active Directory. Example: “CN=Users,DC=domain,DC=com”.
- **Active Directory Group**: The Active Directory group intended for synchronizing users with CYBERQUEST. Default group is PitQeastUsers.
- **ActiveDirectoryIsLdapSecure** - the active directory is secured (0 is LDAP)
- **Active Directory Password**: Account password for the mentioned username which is in **ActiveDirectoryUser**.
- **Active Directory Port**: The port for connecting with Active Directory LDAP service. Default port is 389
- **Active Directory Server** (address): The network IP address of Active Directory domain controller to query
- **Active Directory Suffix**: FQDN of the Active Directory domain
- **Active Directory User**: The administrative user used to connect to Active Directory. Example: “domain\Administrator”. It is also the default user under which CYBERQUEST will perform event collection from Active Directory infrastructure

To edit the setting of this fields you have to press



button, the window will open:



For each setting, press “Save” button to save changes and close the window or press “Cancel” button to close the window without saving changes. As an option, you can close the window without saving changes by clicking the

×

mark in top-right corner.

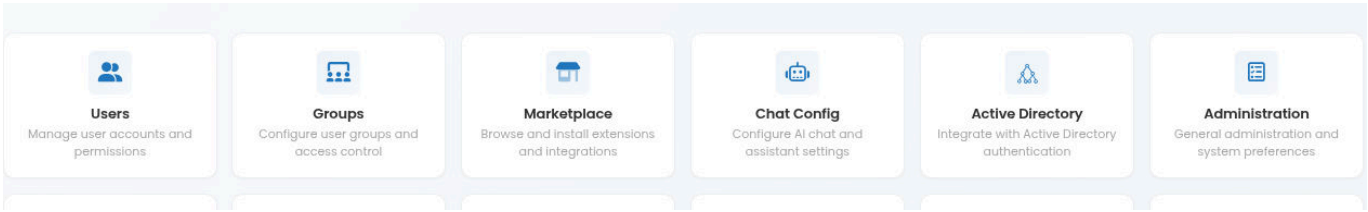
After authentification, every new user has to be added by a CYBERQUEST administrator to their first group. After being added to one or more groups, new users can also be promoted as administrators, if needed.

Configure LDAPS authentication

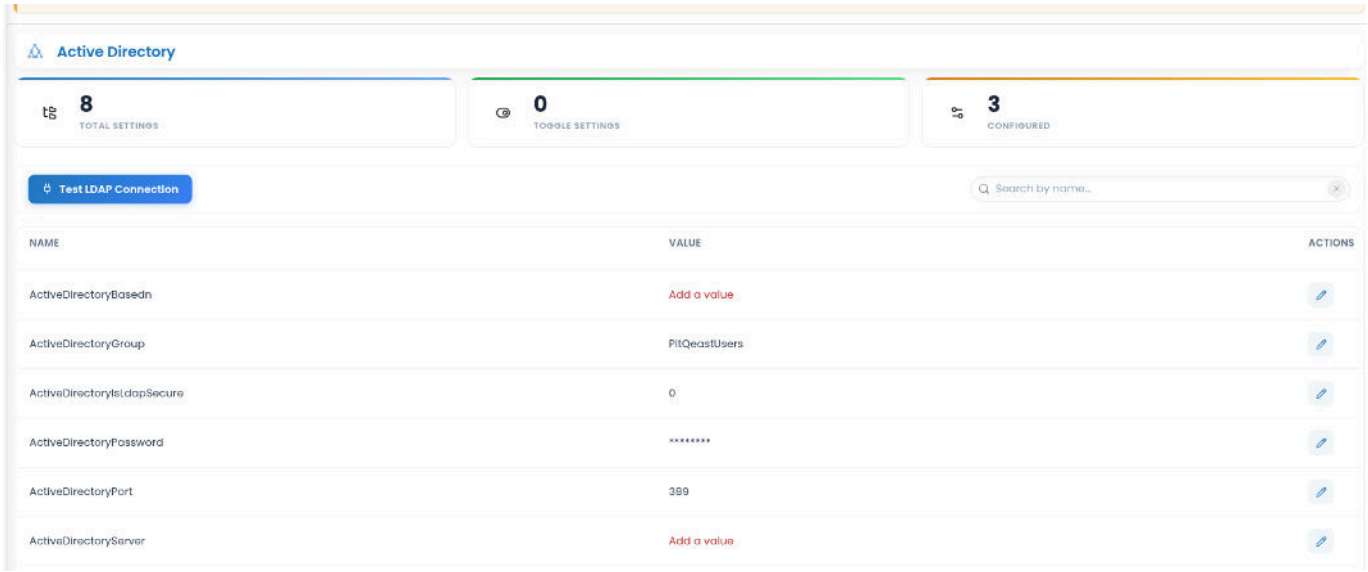
CYBERQUEST can be integrated with Active Directory or LDAPS systems, allowing users to directly authenticate to CYBERQUEST. To do this, please follow these steps:

a. Login to web interface with a user with administrative rights.

b. In web interface select **Settings > Application Settings > Active Directory**.



c. **Active Directory** configuration page opens.



ActiveDirectoryIsLdapSecure - the active directory is secured (1 is for LDAPS)

The server certificate must be imported into the CQ server certificate store, and the certificate must be installed.

If it cannot be installed and has errors, the alternative is to put the certificate created in Windows (client.crt) in the path:

```
etc/ssl/certs/client.crt
```

After that, you have to restart

```
systemctl restart php7.4-fpm.service
```

```
systemctl restart nginx.service
```

The default port for LDAPS is 636.

Configure RADIUS authentication

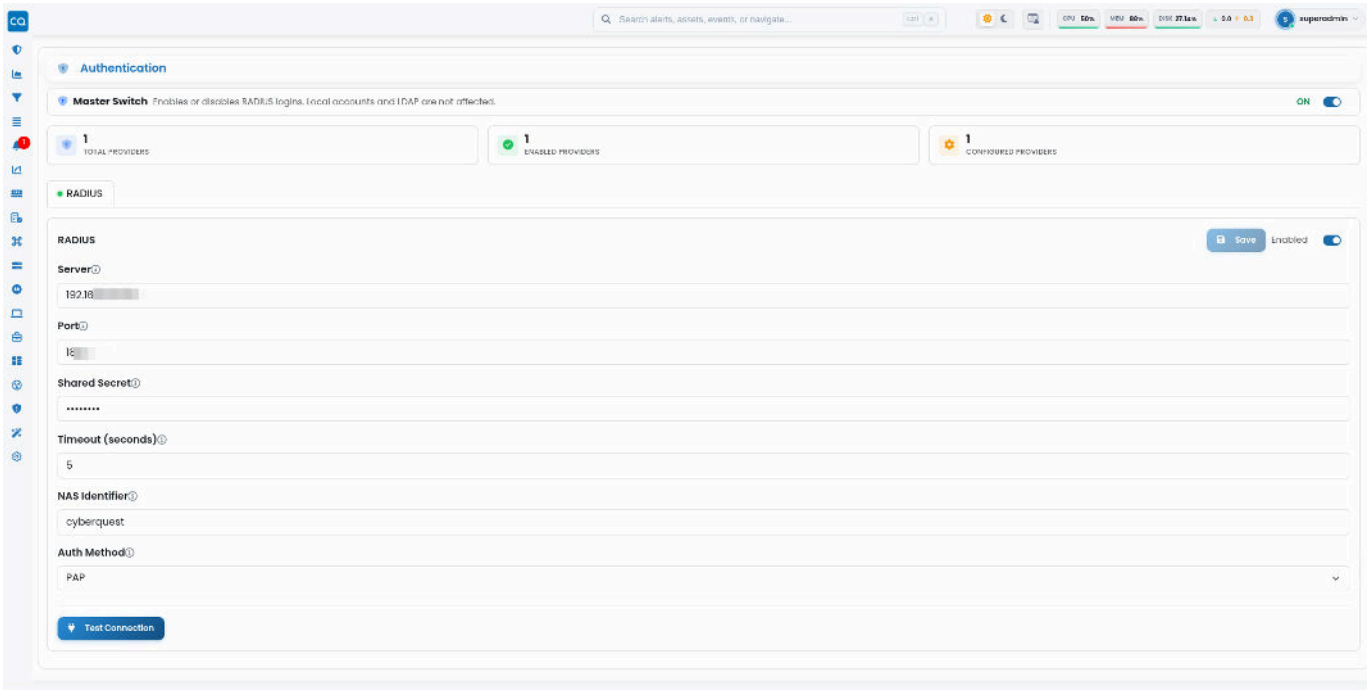
CYBERQUEST supports external user authentication through integration with a RADIUS server. This integration allows user credentials to be validated through the organization's centralized RADIUS authentication infrastructure.

To configure RADIUS authentication, follow these steps:

a. Log in to the CYBERQUEST Web Interface using an account with administrative privileges.

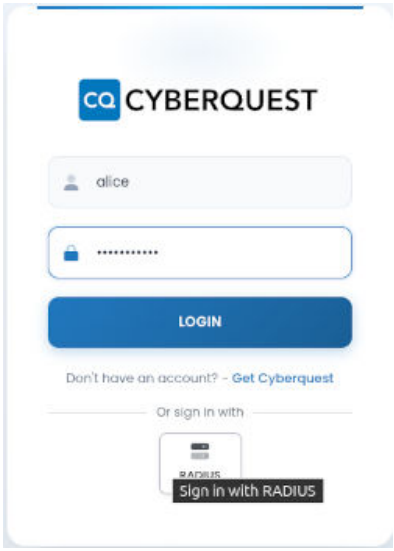
b. Open the RADIUS authentication configuration page from the application settings.

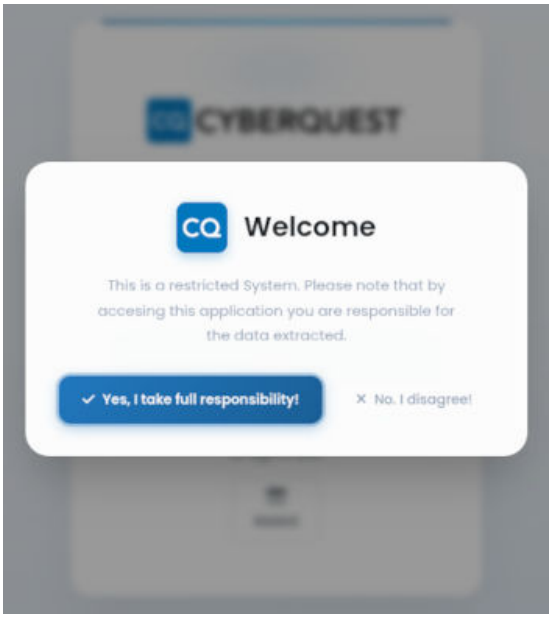
c. Configure the connection parameters of the external RADIUS server and enable RADIUS authentication.



d. Save the configuration.

Once RADIUS authentication is enabled, the **RADIUS** option becomes available on the CYBERQUEST authentication page. Users enter their credentials and select **RADIUS**, after which the authentication request is validated by the configured external RADIUS server.

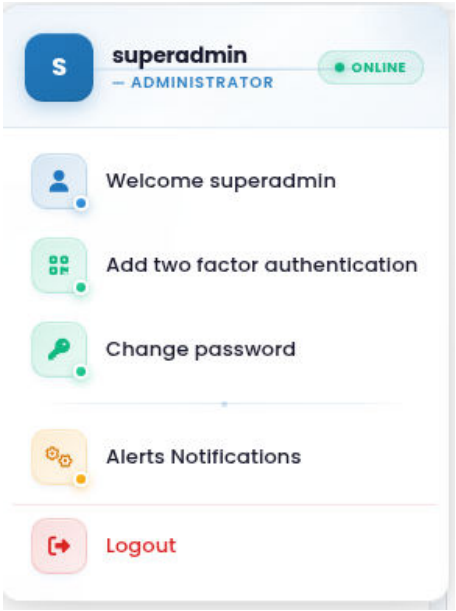




Add two factor authentication

With two-factor authentication (2FA), you add an extra layer of security to your account. In addition to your password, you'll also need a code generated by Google Authenticator on your phone.

From **User actions** menu, select **Add two factor authentication**:



To see how to activate 2FA, please follow the links below:

How to enable two-factor authentication (2FA) to an user account, please access the link: How to enable two-factor authentication (2FA) to an user account.

How to disable two-factor authentication (2FA) to an user account, please access the link: How to disable two-factor authentication (2FA) to an user account.

Licensing

CYBERQUEST license

CYBERQUEST is available both as a free edition or as a commercial edition. The commercial editions are: **Logger, Light**, **Advanced**, **Enterprise** and **Ultimate**. The table below details the features of each edition:

Description / version	Free	Logger	Light	Advanced	Enterprise	Ultimate
Users limit	1	3	5	10	20	Unlimited*
Included cores	4	4	4	6	8	1**
Included EPS	250	250	500	750	1000	Unlimited*
Daily GB of data	1	2	10	160	600	Unlimited*
CPU cores/instance	4	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
Dashboards	yes	yes	yes	yes	yes	yes
Custom dashboards	no	no	yes	yes	yes	yes
Dashboards per dashgroup	6	9	12	15	24	Unlimited*
Dashgroups per instance	2	4	6	10	16	Unlimited*
Data permissions-no. of filters	×	×	2	10	Unlimited*	Unlimited*
Short term Data Storage (days)	15	30	30	90	Unlimited*	Unlimited*
Long term Data Storage (days)	×	×	365	730	Unlimited*	Unlimited*
Max. no. of Online DataStorage Nodes/instance	1	1	2	3	Unlimited*	Unlimited*
Max. no. of DTS Objects	4	6	10	15	Unlimited*	Unlimited*
Geolocation	☑	☑	☑	☑	☑	☑
Reports	☑	☑	☑	☑	☑	☑
Compliance Reports	☑	☑	☑	☑	☑	☑
Asset Management	×	×	×	☑	☑	☑
Windows Agent Collection	☑	☑	☑	☑	☑	☑
ODBC Data Collection	☑	☑	☑	☑	☑	☑
Syslog Data Collection	☑	☑	☑	☑	☑	☑
NetFlow Data Collection	×	×	×	☑	☑	☑
NetFlow Stitching	×	×	×	×	☑	☑
Multiple Data server for advanced technologies	×	×	×	☑	☑	☑
MultiTenancy	×	×	×	×	×	☑
Simple Alerts (1 step rules)	×	×	20	50	Unlimited*	Unlimited*

Description / version	Free	Logger	Light	Advanced	Enterprise	Ultimate
Correlated Alerts (multi step rules)	✕	✕	5	20	Unlimited*	Unlimited*
Summary Alerts	✕	✕	✕	20	Unlimited*	Unlimited*
Add-on 2, 4 or 8 Cores-extra fee	✕	☑	☑	☑	☑	☑
Add-on 1GB, 5GB, 10GB or 100 GB/day-extra fee	✕	☑	☑	☑	☑	n/a

***No limit is set in the license for the number of integrated IT&C devices/data sources. Performance and processing capacity depend on the allocated hardware resources**

****The license is for 1 CPU. Minimum numbers of license cores that can be purchased is 8 and the estimated performance is about 1800 EPS**

To see how CYBERQUEST license is working and how to add a new license, please follow the link: How CYBERQUEST license works.

Set-up

Installation

Minimum system requirements

Server minimum system requirements

CYBERQUEST is a virtual appliance but can be installed as a physical appliance as well.

In order to install CYBERQUEST 2.30 physical or virtual machines must be provided. CYBERQUEST 2.30 resides on a Linux Debian 11 instance.

- For all CYBERQUEST residing virtual machines resources must be reserved (CPU cores and RAM).
- For CYBERQUEST best performance 6th gen Intel CPU's or equivalent must be provided.

Minimum recommended resources, as per the standard versions (no add-ons installed and for CYBERQUEST 2.30 Ultimate - 8 CPU cores license) are:

Version of CYBERQUEST 2.20	Minimum RAM recommended	Minimum Storage Recommended - GB (for data only)
Logger	8*	100**
Light	8*	200**
Advanced	16*	500**
Enterprise	32*	1000**
Ultimate	32*	1000**

***This is the minimum recommended RAM to be granted to virtual machines hosting CYBERQUEST instances. As the solutions may scale, higher RAM capacity must be allocated. For such situations, a certified CYBERQUEST technician must be consulted.**

****This is the minimum recommended storage capacity - for data only. The retention period (data availability for hot searches and archive) is directly proportional with the storage capacity. For situations where online and offline data must cover longer periods, a certified CYBERQUEST technician must be consulted in order to provide requirements for storage capacity.**

User(client) web application minimum system requirements:

- Web Browsers: Firefox (86+), Chrome (83+)
- Resolution: Full HD Display (1980x1080)

Windows collector (agent)

- .Net Framework 4.8
- Windows Server operating System (2012+) x64 operating system
- Visual C++ redistributable 2019+

Supported virtual enviroments

VMware is a virtualization computing software. With VMware server virtualization, a hypervisor is installed on the physical server to allow for multiple virtual machines (VMs) to run on the same physical server. Each VM can run its own operating system (OS), which means multiple operating systems can run on one physical server. All the VMs on the same physical server share resources, such as networking and RAM.

Hyper-V is Microsoft's hardware virtualization product, each virtual machine runs on virtual hardware. Hyper-V runs each virtual machine in its own isolated space, which means you can run more than one virtual machine on the same hardware at the same time. Hyper-V allows you to create virtual hard drives, virtual switches and a host of other virtual devices, all of which can be added to virtual machines.

AIO

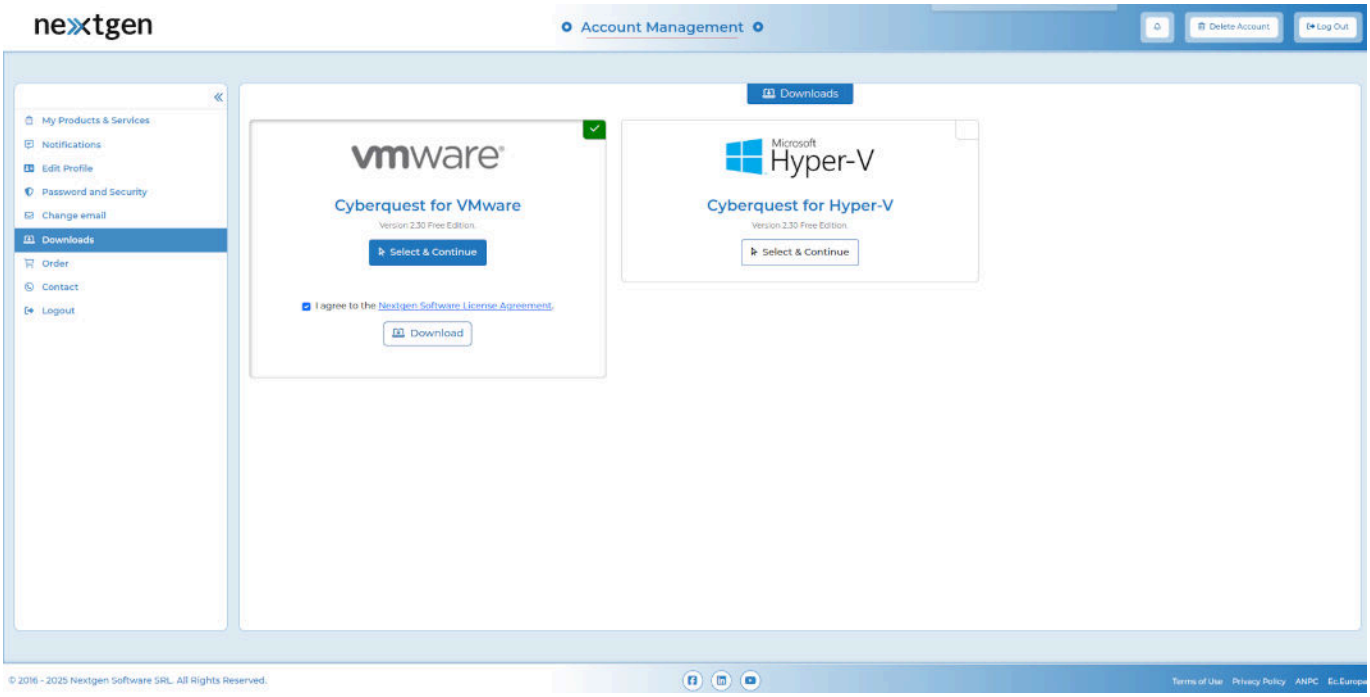
Installation for VMware

Prior installation system requirements

In order to configure the virtual machine, the following requirements must be met first:

- ESXi 8.0 or later;
- 4 CPU cores;
- Minimum 32 GB RAM (64 GB recommended);
- Minimum 60 GB Storage;

Download the CYBERQUEST server by registering on the portal here (https://portal.cyberquest.cloud/login), navigating to the Downloads section, selecting *Cyberquest for VMware*, agreeing to the license terms, and clicking the Download button.



Installing CYBERQUEST

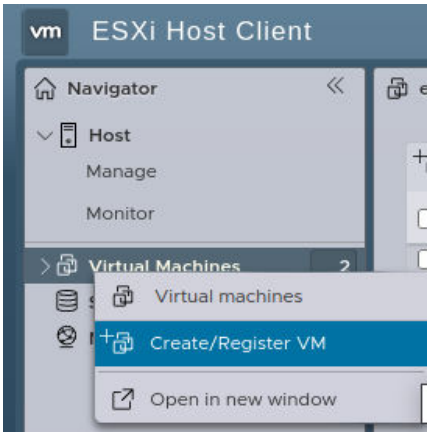
A. OVA Deployment

For deploying the CYBERQUEST virtual machine (OVA file), follow these steps:

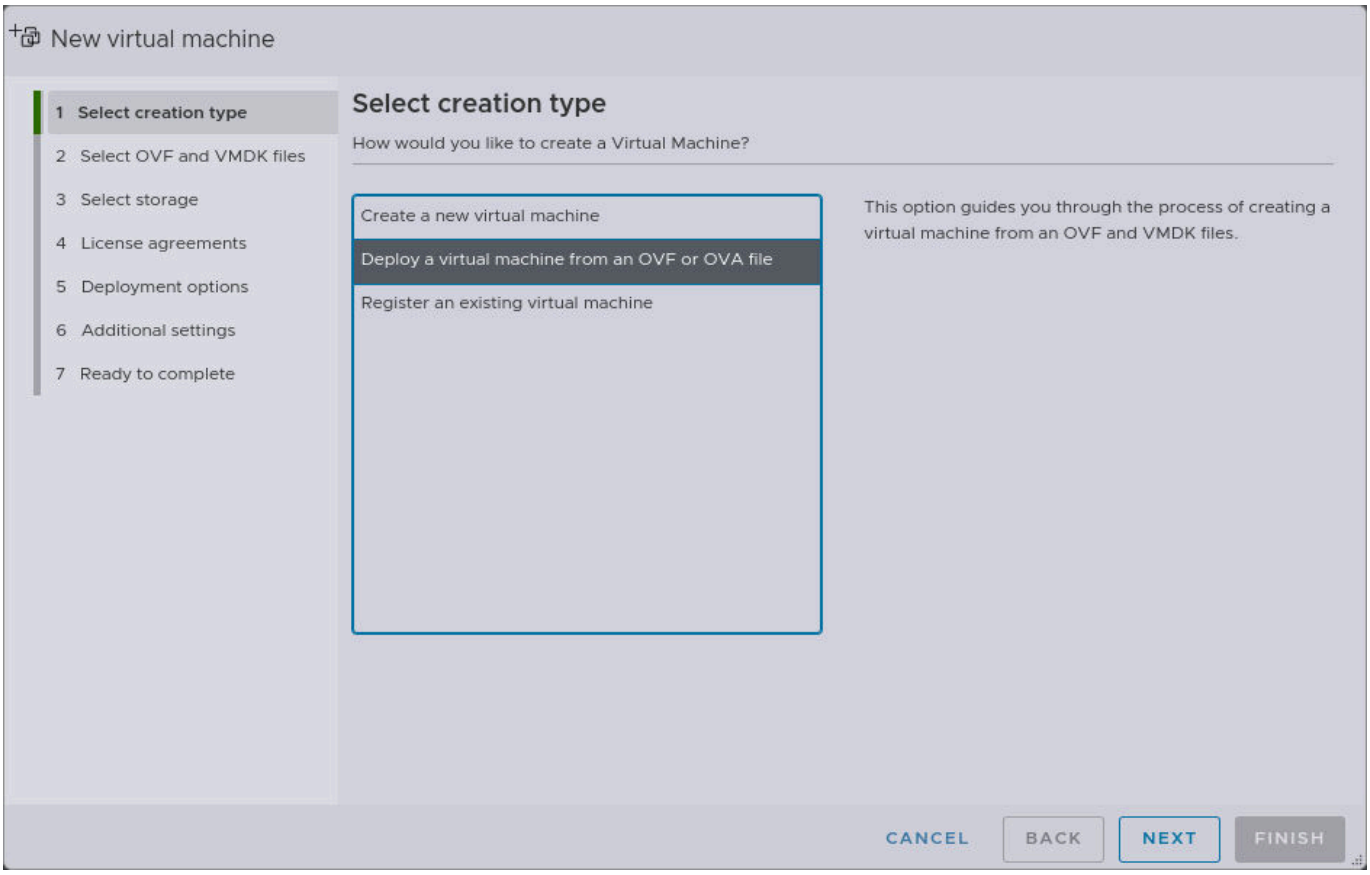
1.Connect to vCenter (or ESXi Hypervisor). Open vSphere Client or the web interface. Fill in the username and password credentials.



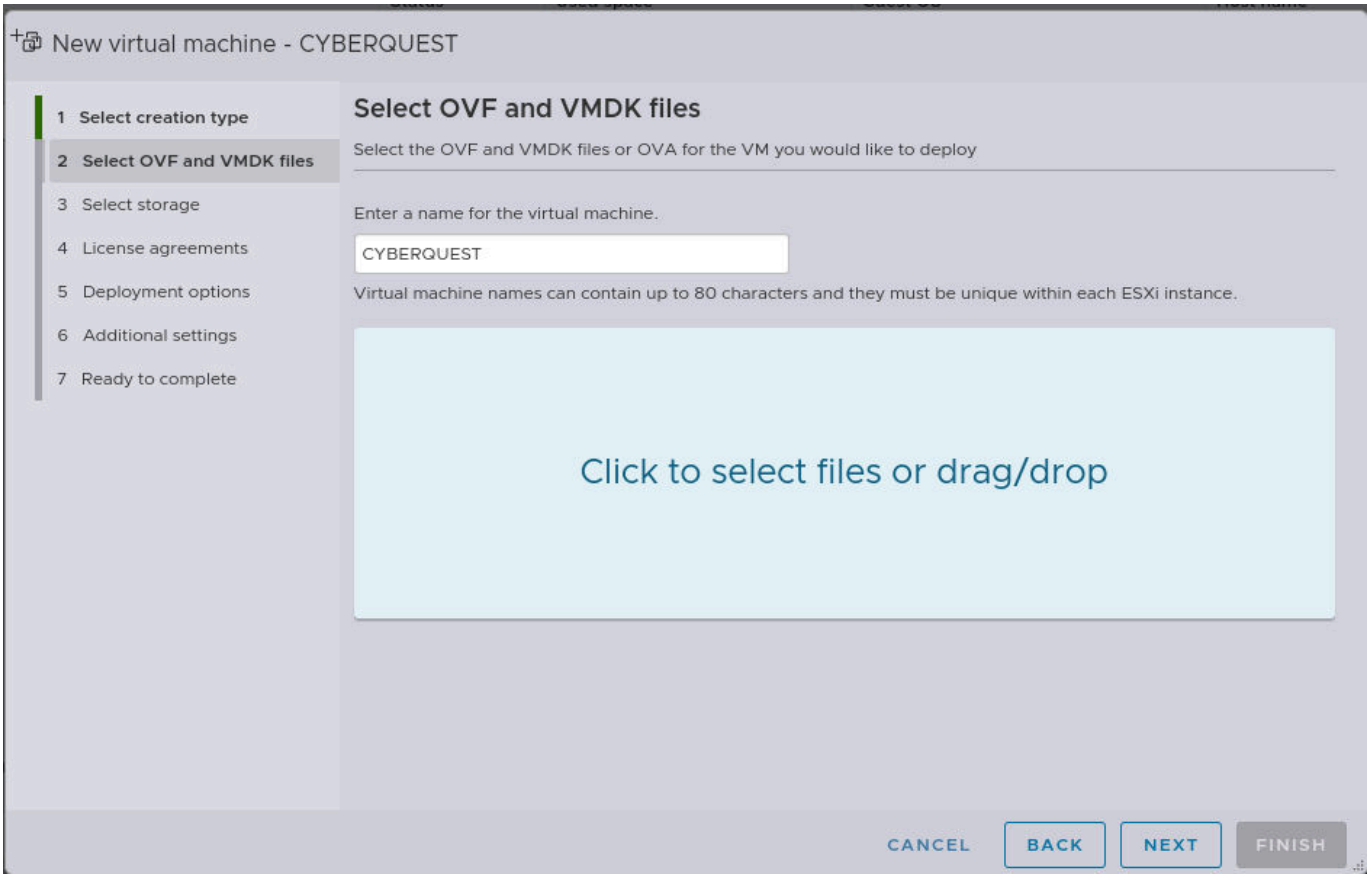
2.Right click on **Virtual Machines** and select **Create/Register VM**



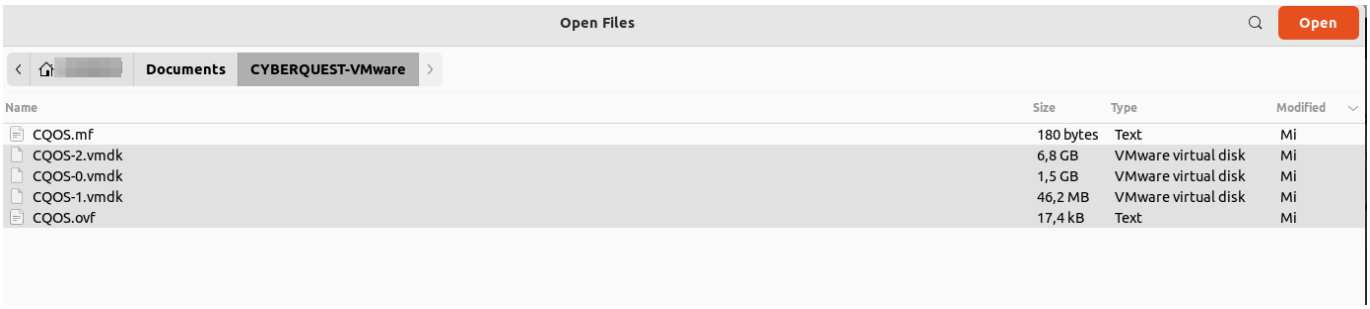
3.In this window, select **Deploy a virtual machine from an OVF or OVA file** and click on **Next**

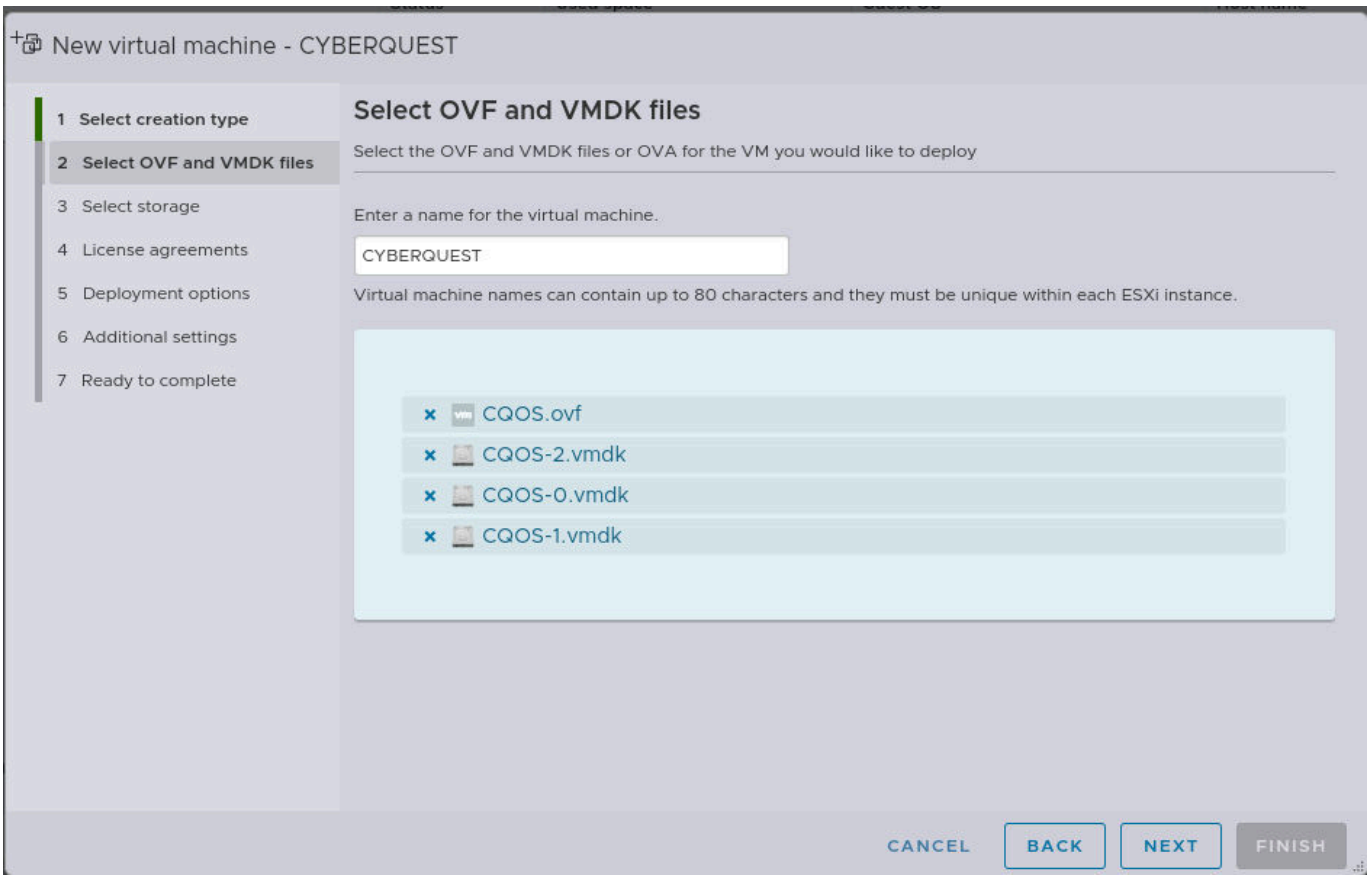


4.Name the virtual machine (e.g., **CYBERQUEST**), and click on **Click to select files or drag/drop** to select files for CYBERQUEST server deployment.

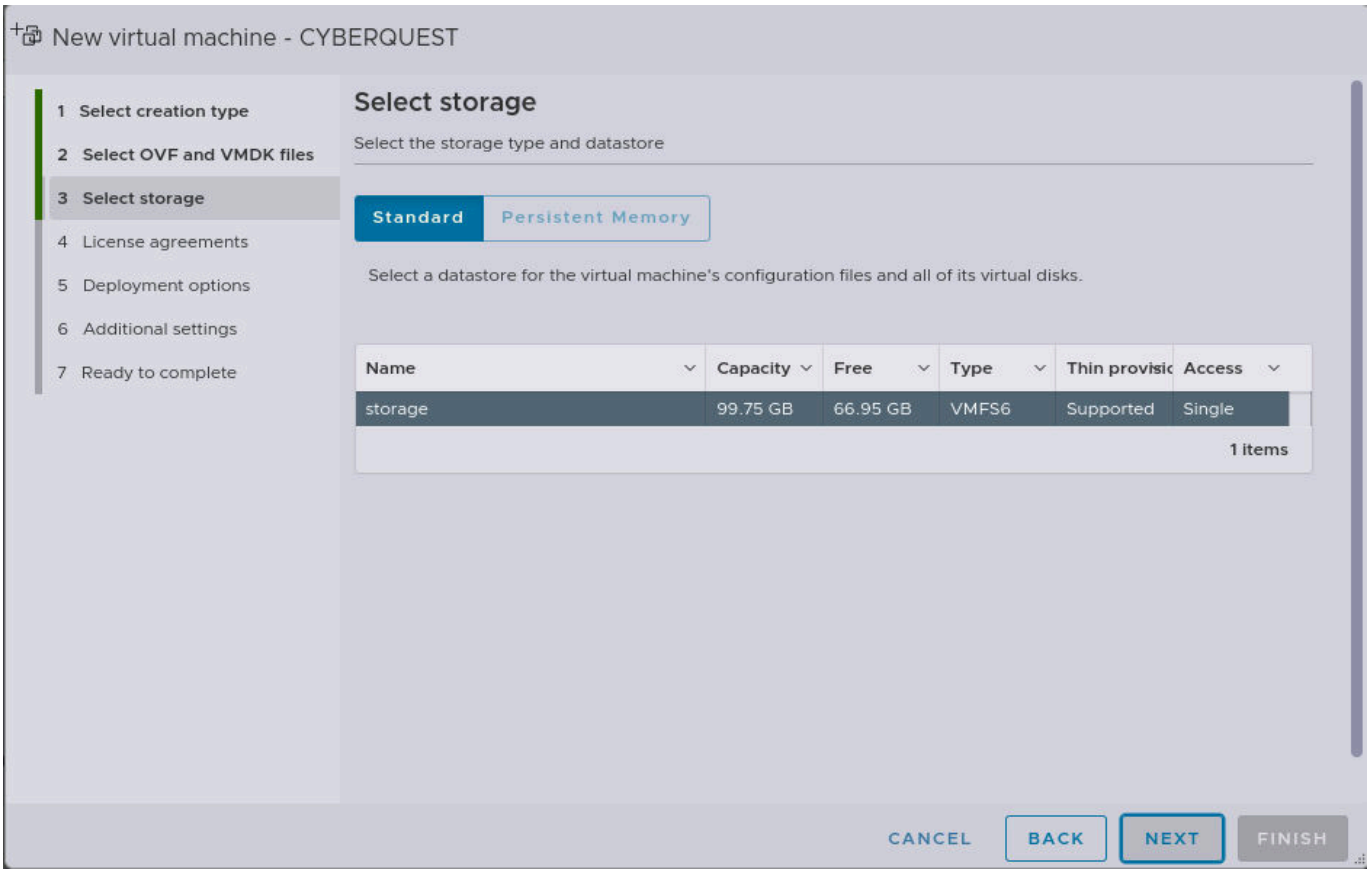


5.In the new window, locate the CYBERQUEST virtual machine, select the files and click **Open** > **Next**.

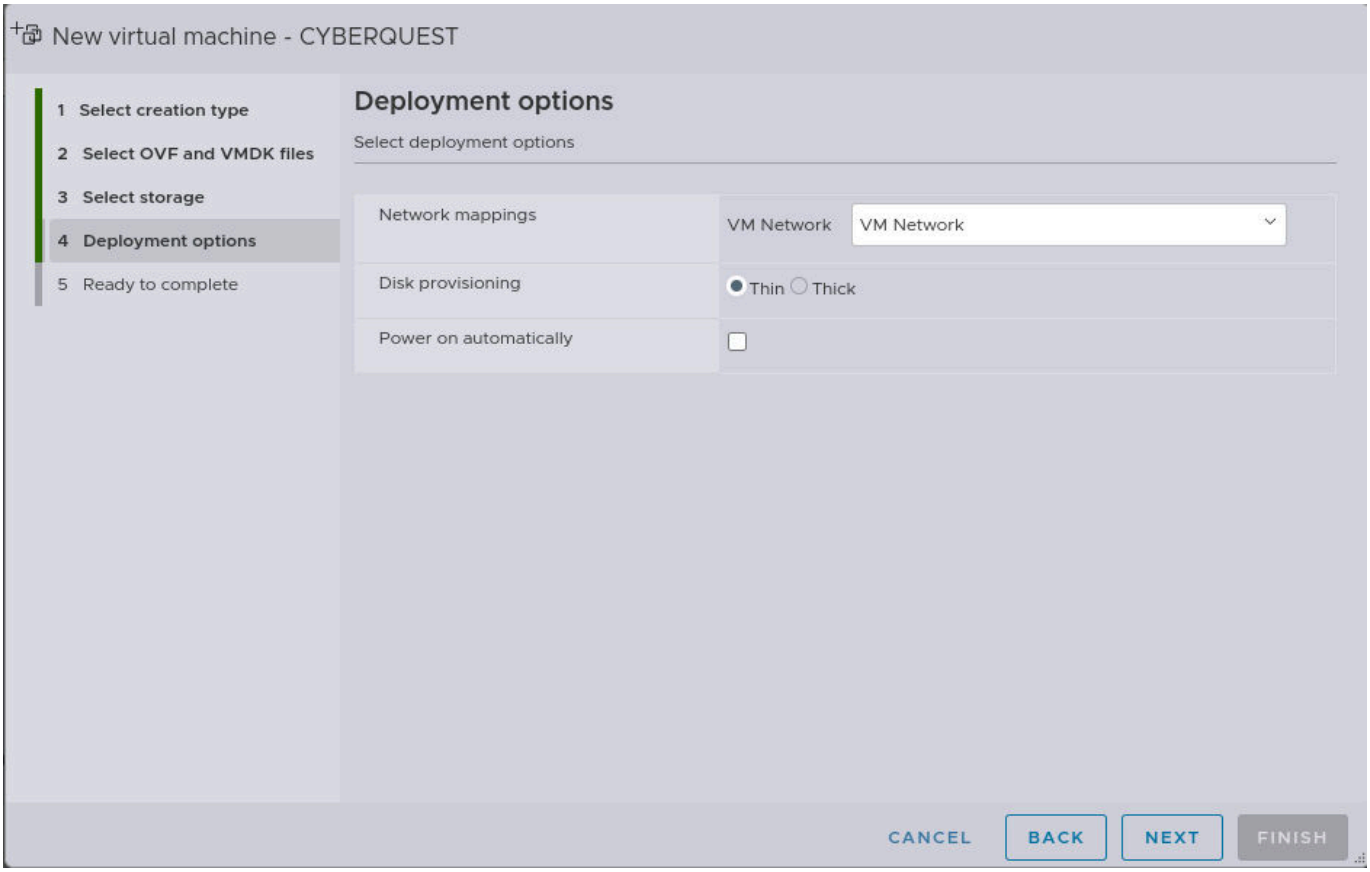




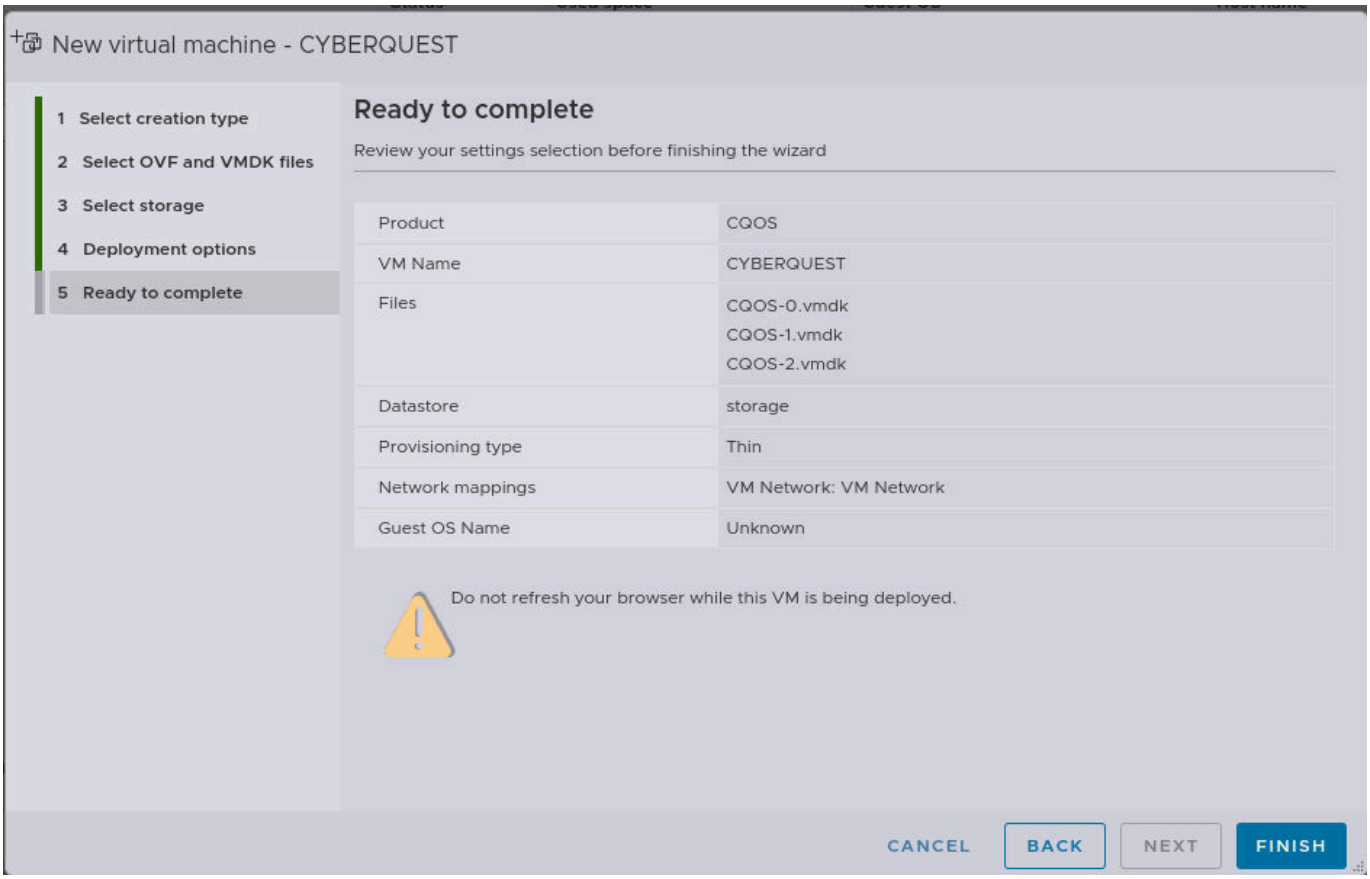
6.Select the storage location for importing the virtual machine, then click **Next**.

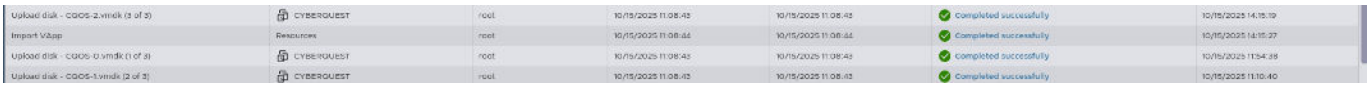


7.Select the network and check the box for **Thin** in **Disk provisioning**, then click **Next**.



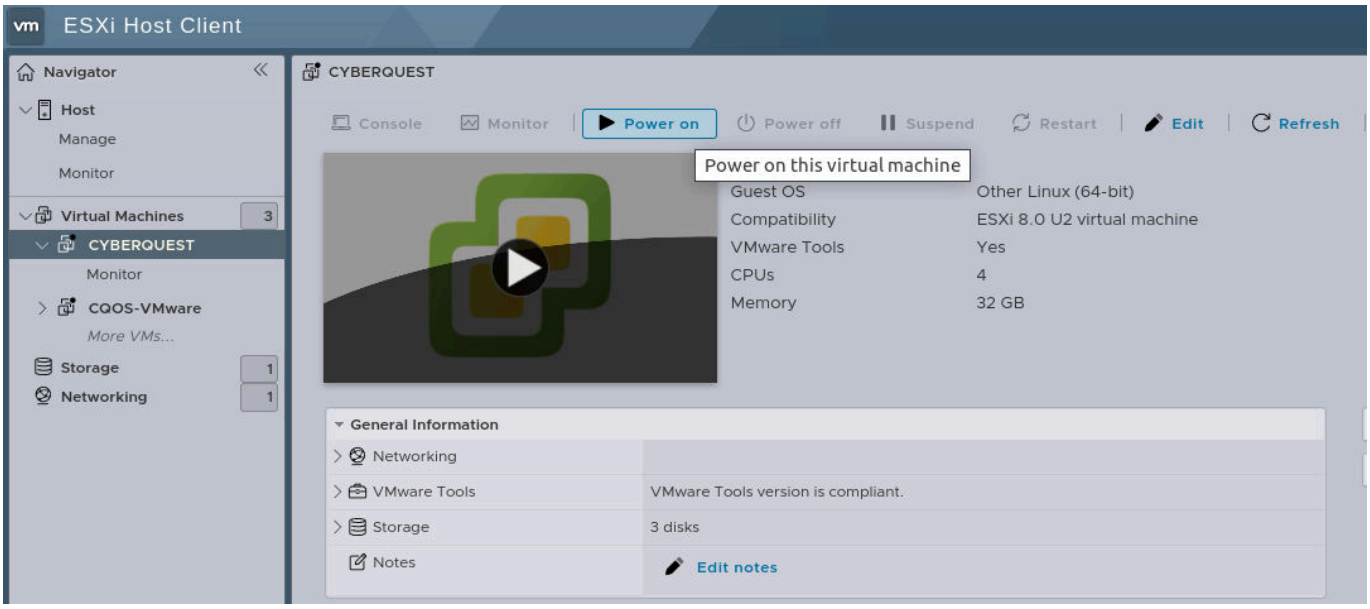
8.Review the previously selected parameters, click **Finish** and wait for the import of CYBERQUEST virtual machine to be complete.



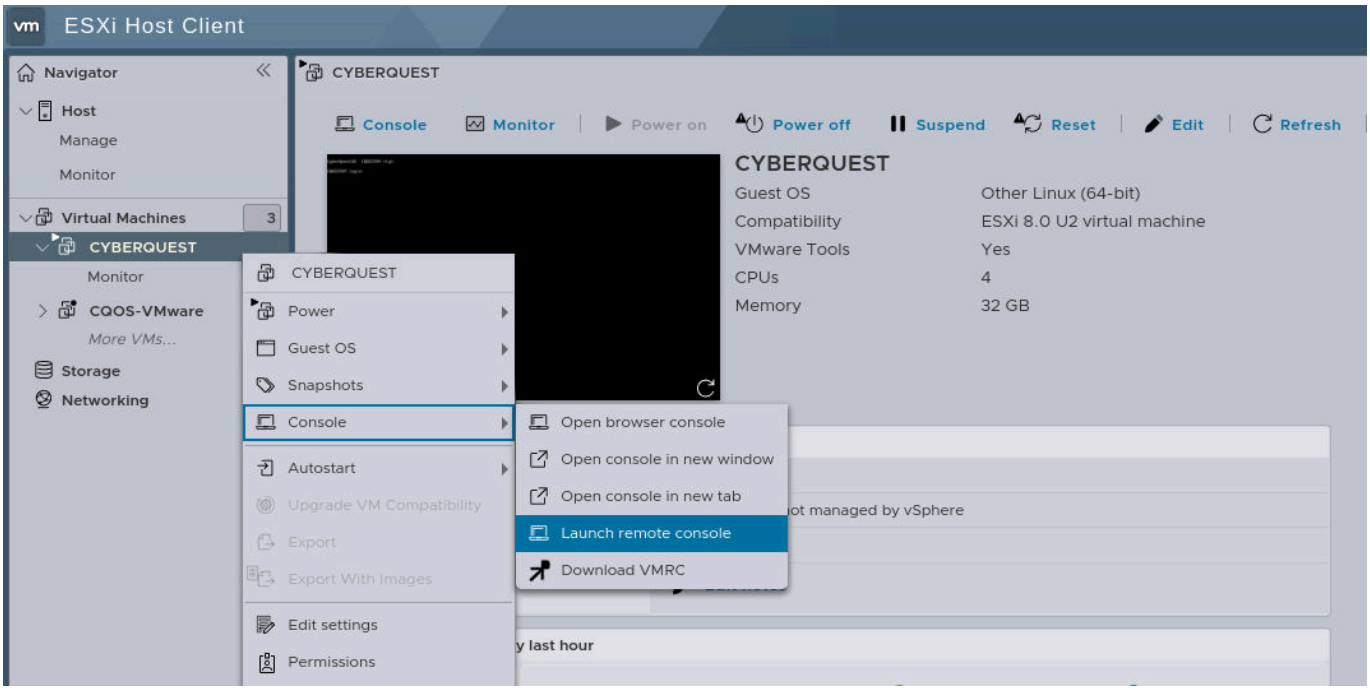


B. CYBERQUEST virtual machine configuration

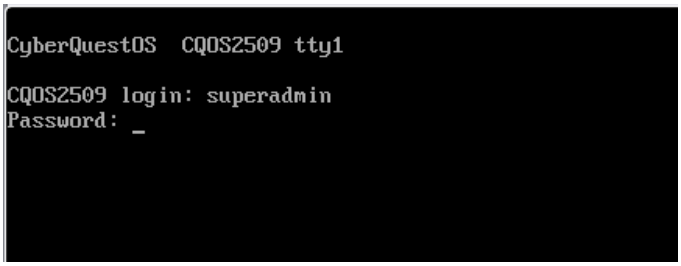
1.Start the CYBERQUEST virtual machine using the vSphere client (or the web interface) by selecting the **Power on** button in the top menu.



2.To open the console, right-click the **virtual machine**, then select **Console** > **Launch Remote Console**. The **Console** button in the menu can also be used.

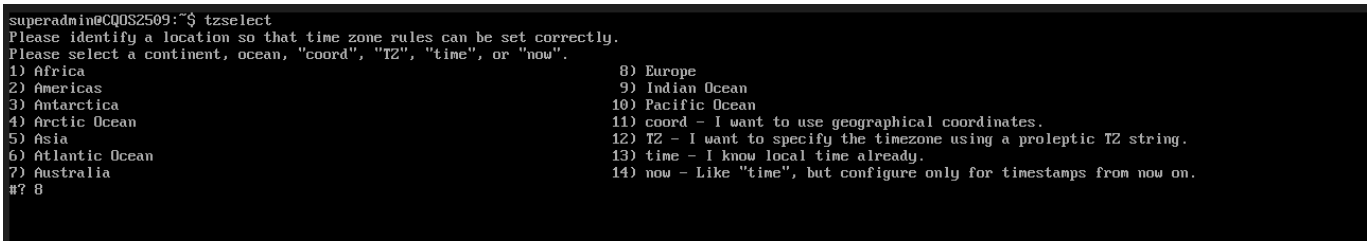


3.Connect using the username "**superadmin**" and password "**toor1**".



4.To set the TimeZone, use the following command and follow the interactive steps:

```
tzselect
```







5.Configure the network by running the command and setting the Static IP:

```
sudo nano /etc/netplan/def.yaml
```

To apply the network configurations run this command:

```
sudo netplan apply
```

6.The services start automatically. If they fail to start, log in as root, navigate to the *cyberquest-deployment* directory, and run the following command:

```
systemctl start cyberquest-deployment.service
```

Check that the services have started by running the following command:

```
docker ps -a
```

Installation for Hyper-V

Prior installation system requirements

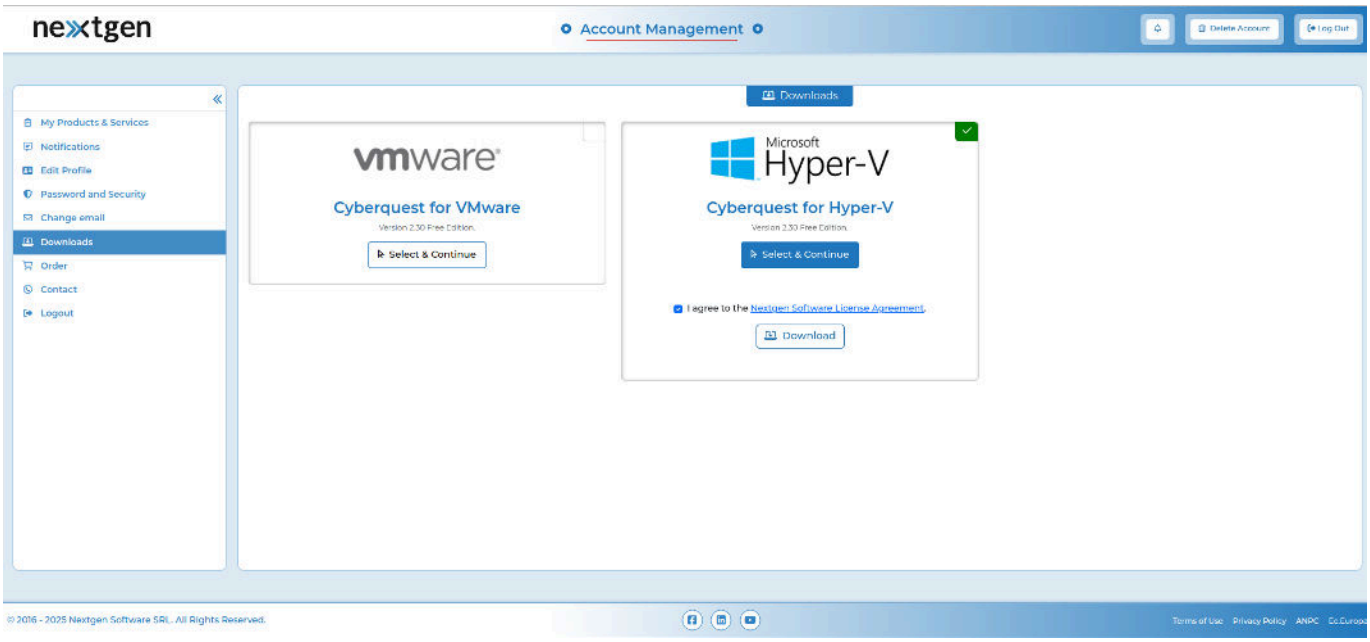
In order to configure the virtual machine, the following requirements must be met first:

- HyperV (minimum Windows 2016);
- VM Gen 1 compatible;
- 4 CPU cores;
- Minimum 32 GB RAM (64 GB recommended);
- Minimum 60 GB Storage;

Deployment Guide for Hyper-V

To deploy the CYBERQUEST server in a Hyper-V environment do the following steps:

Step 1: Download the CYBERQUEST server from here (https://portal.cyberquest.cloud/login). Register and click on **Downloads** section and after select **Cyberquest for Hyper-V**, and press **Download** button.



Step 2: Extract the content of the archive

Step 3: Open **Hyper-V Manager** from **Start > Windows Administrative Tools**

CYBERQUEST server can be deployed by create a virtual machine and attach the 3 virtual disks.

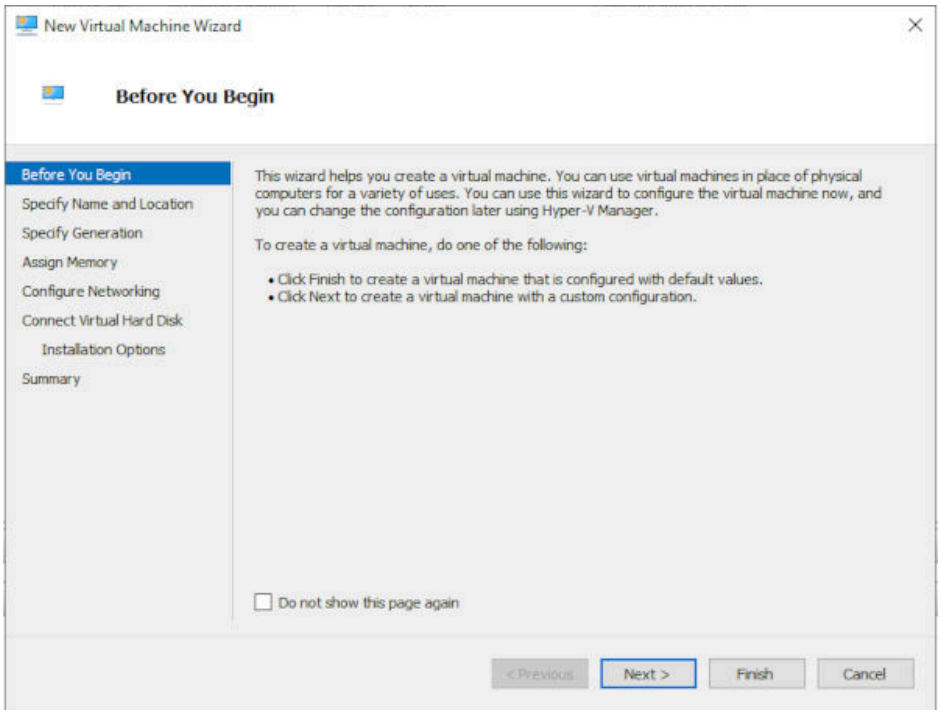
Create a virtual machine and attach the CYBERQUEST virtual disks

A. To create CYBERQUEST virtual machine please follow the steps from bellow:

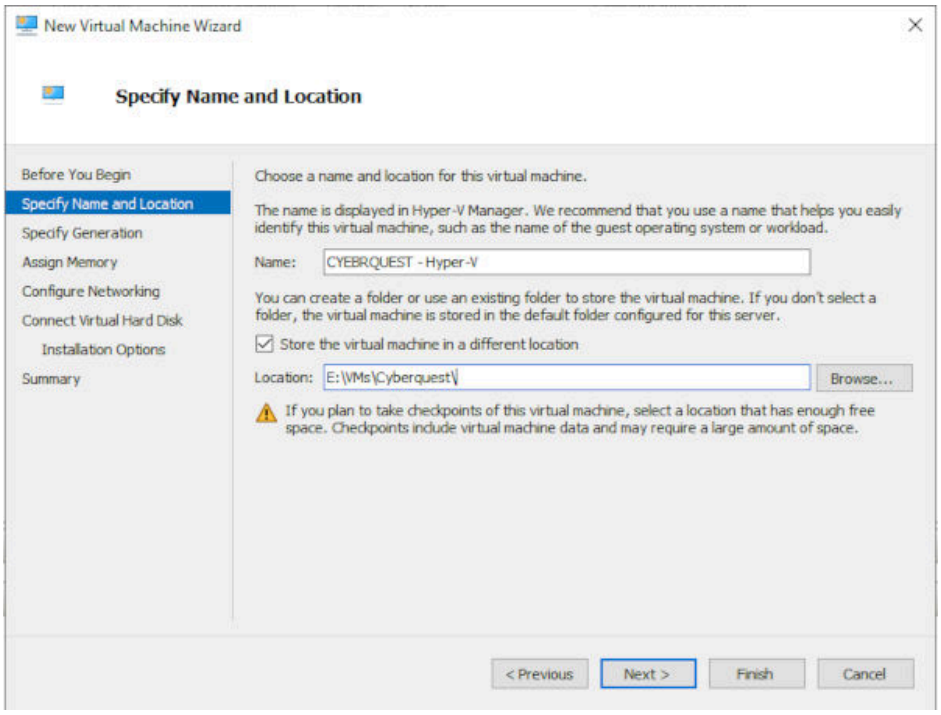
1.In the top-left corner, right-click the Hyper-V server and select: **New > Virtual Machine**.

![Alt Image](./images/installation/200 (26).png)

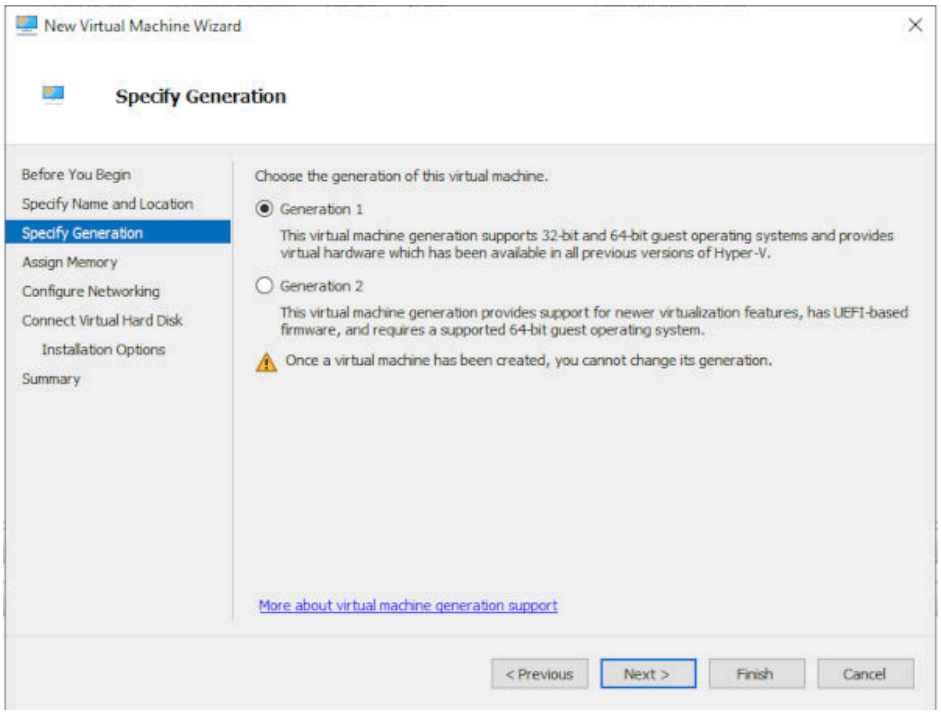
2.In the **Before You Begin** section, click **Next**.



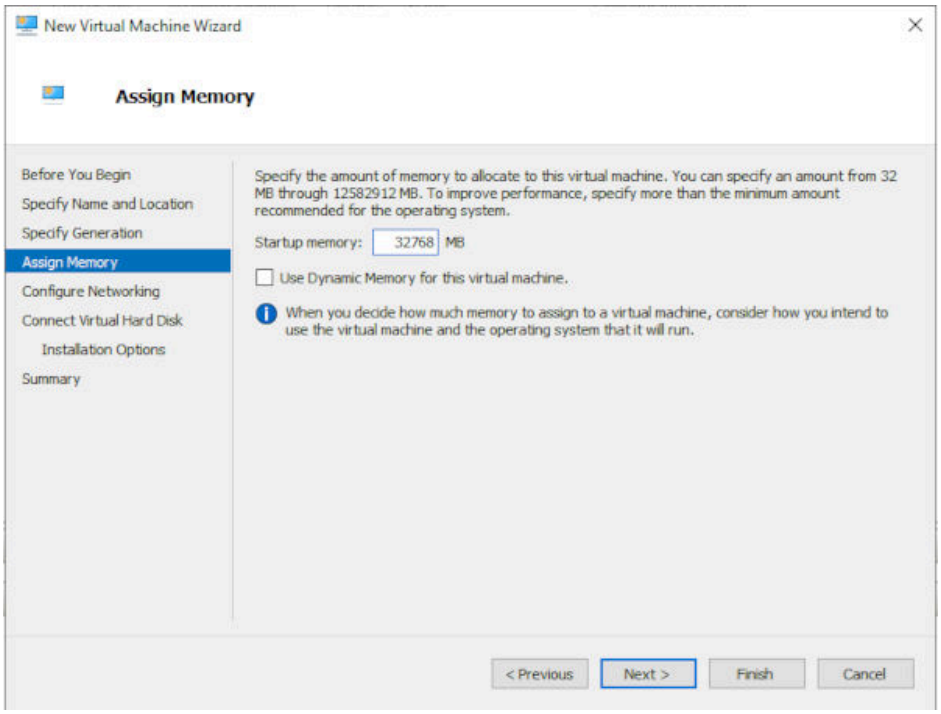
3.In the **Specify Name and Location** section, provide a name for the CYBERQUEST server and choose the folder to store the virtual machine.



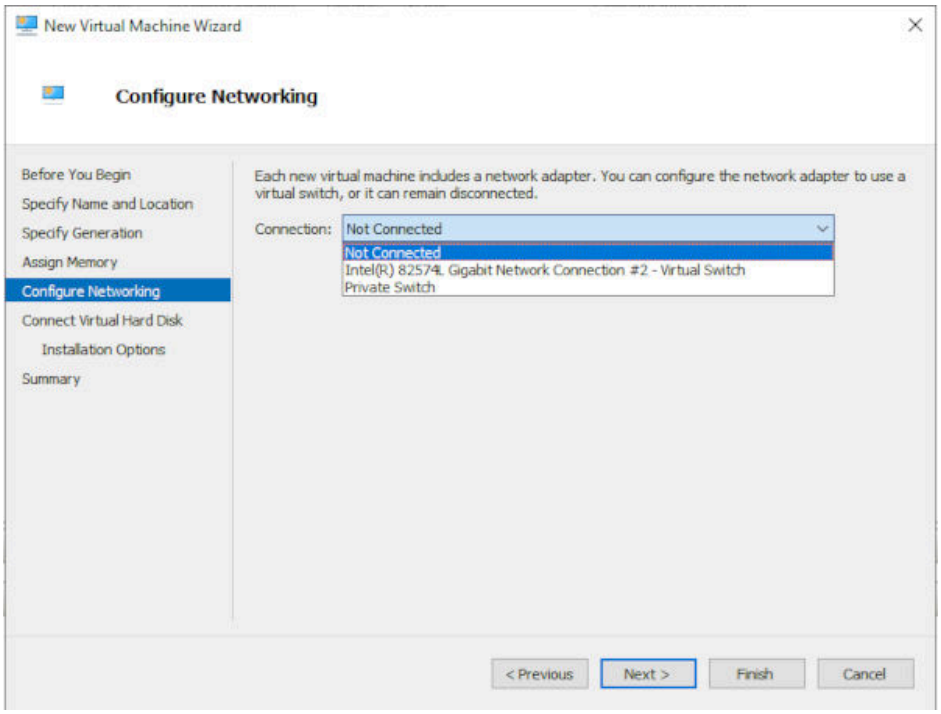
4.In the **Specify Generation** section, select the appropriate Generation type for the environment and click **Next**.



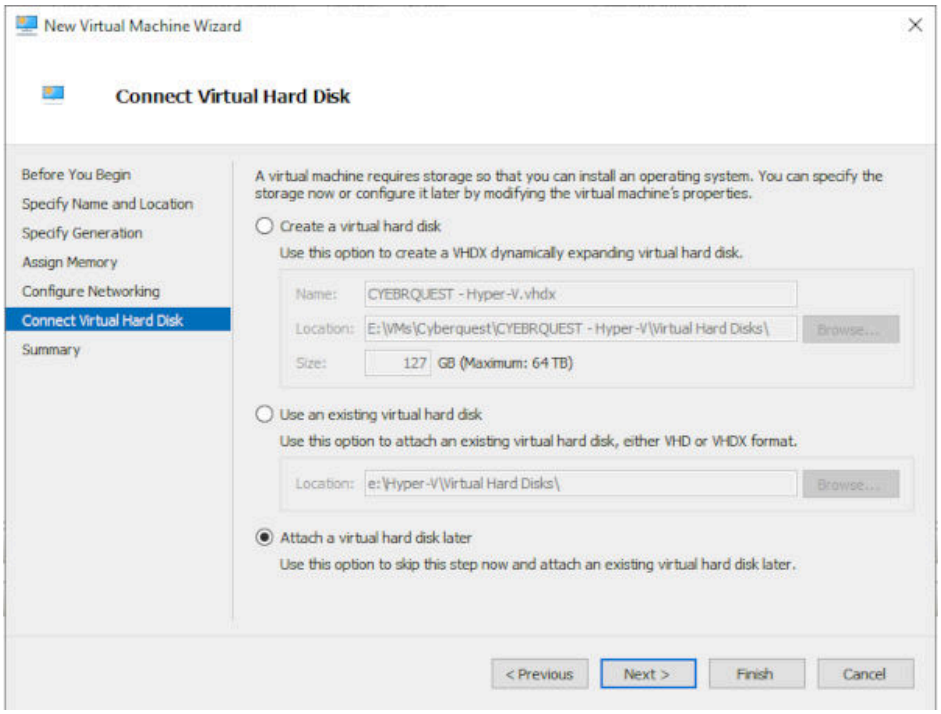
5.In the **Assign Memory** section, enter the RAM amount for the CYBERQUEST server and click **Next**.



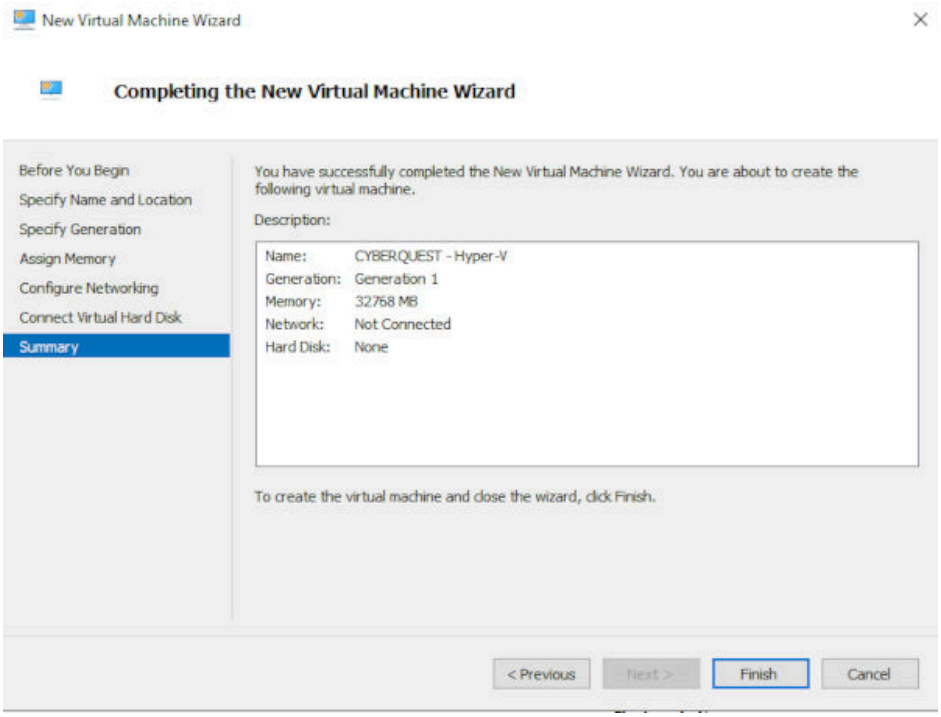
6.In the **Configure Networking** section, choose the network switch and click **Next**



7.In the **Connect Virtual Hard Disk** section, select **Attach a virtual hard disk later** and click **Next**

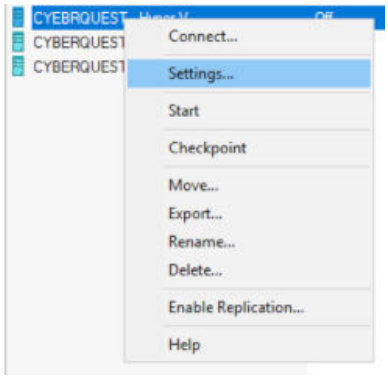


8.In the **Summary** section, click **Finish**

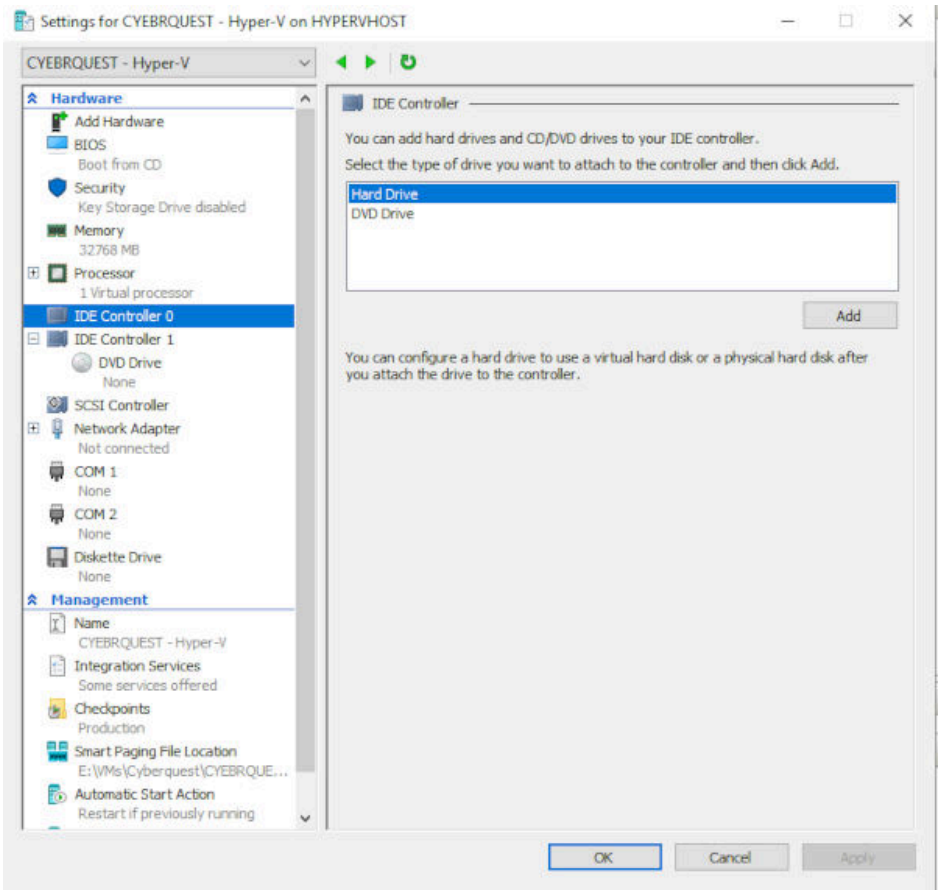


B. To attach the CYBERQUEST virtual disks, follow the steps below:

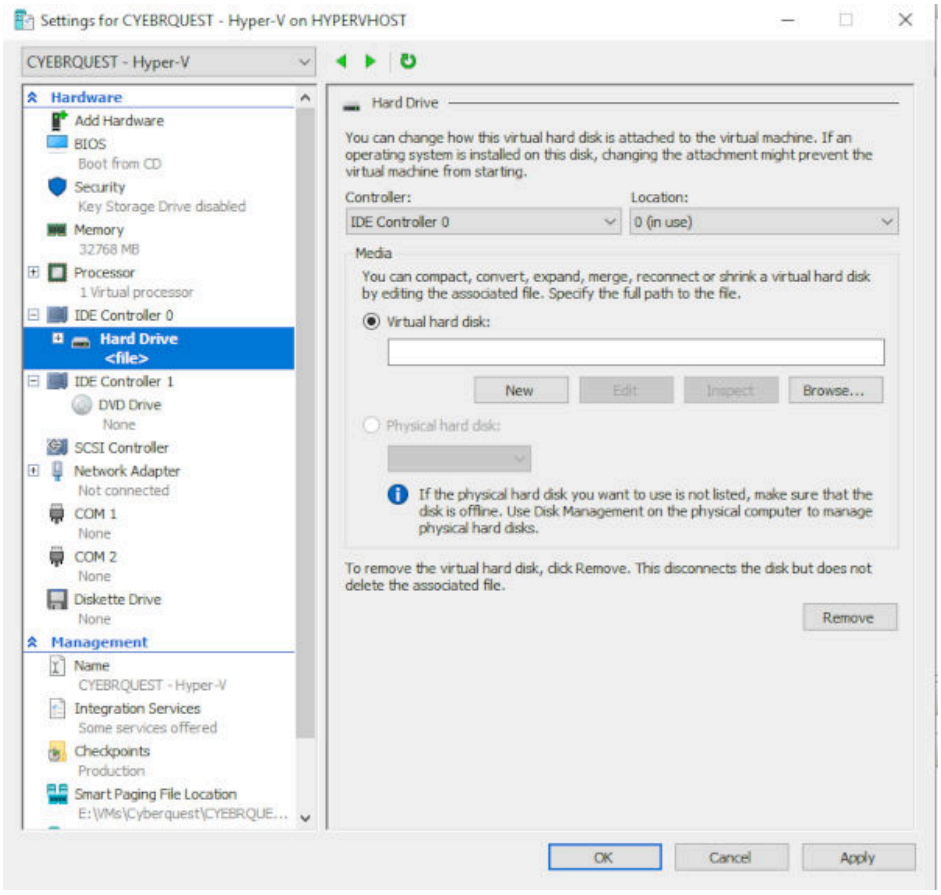
1.Right-click the created Virtual Machine and select **Settings**.



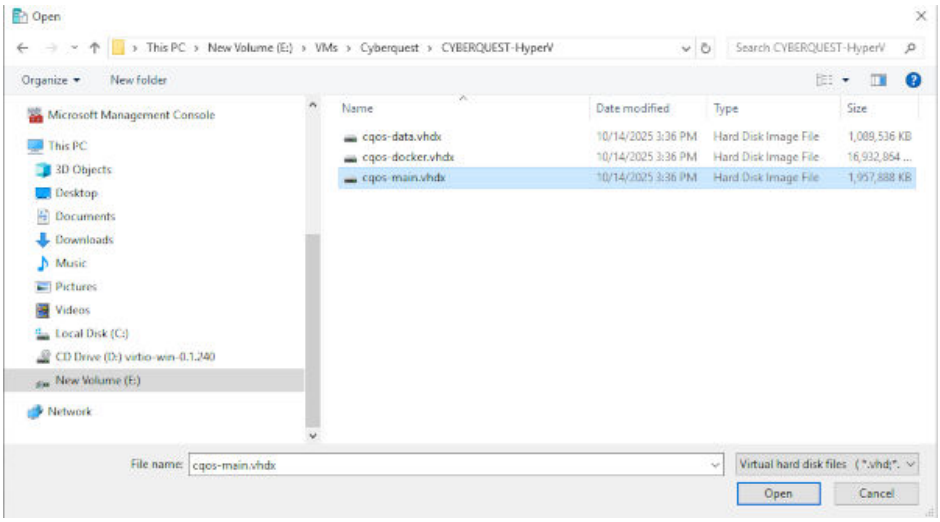
2.In the **Settings** window select **IDE Controller 0**. In the right side select **Hard Drive** option and click **Add**

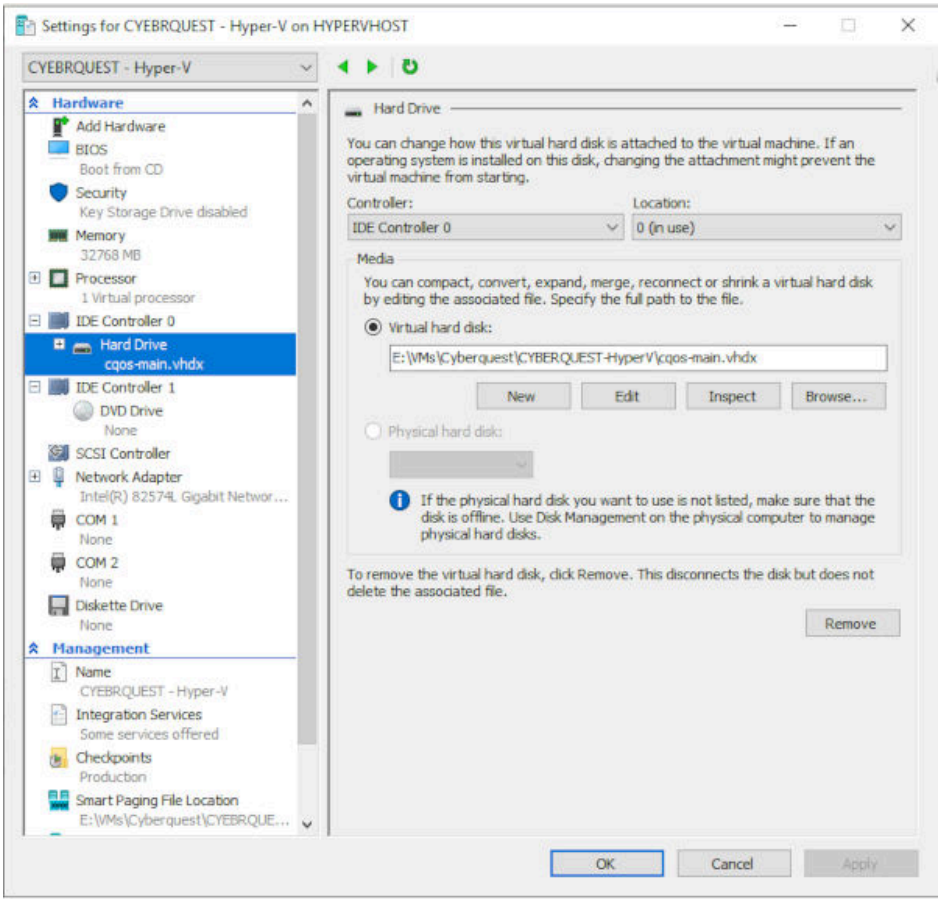


3.In the **Media** section, click **Browse** and navigate to the location where the CYBERQUEST server virtual hard disks are stored.

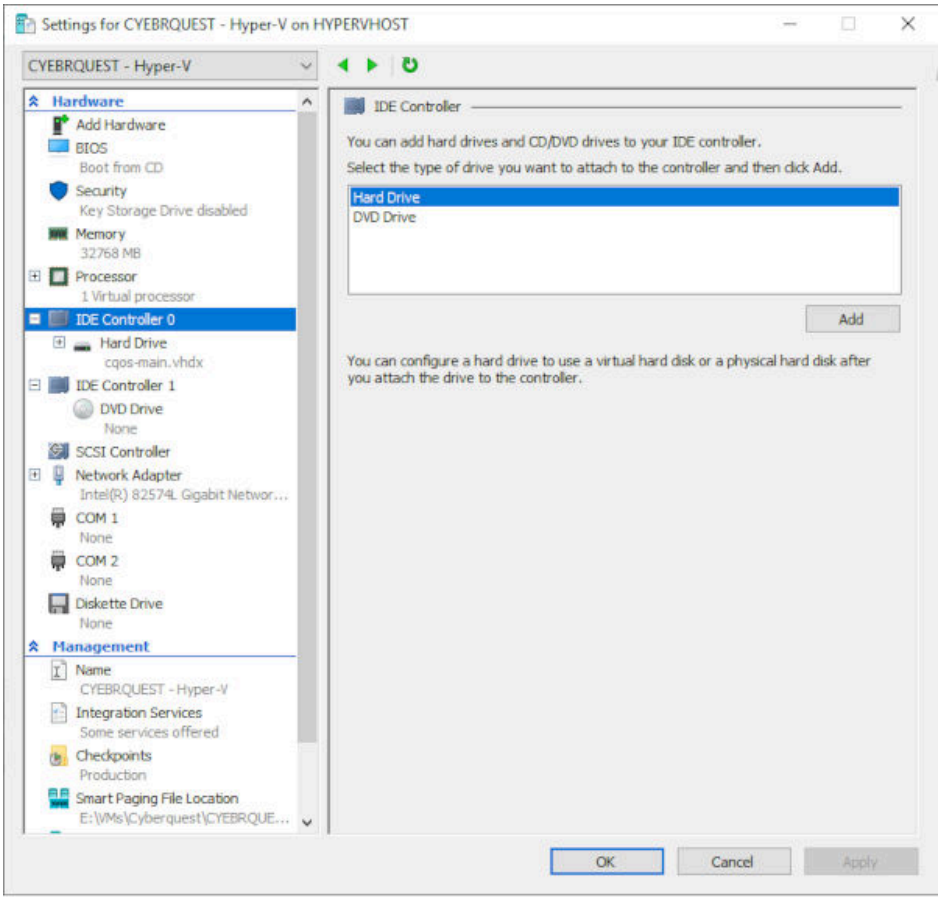


4.Select the **first disk file** *cqos-main.vhdx*, and after click **Open** and **Apply**

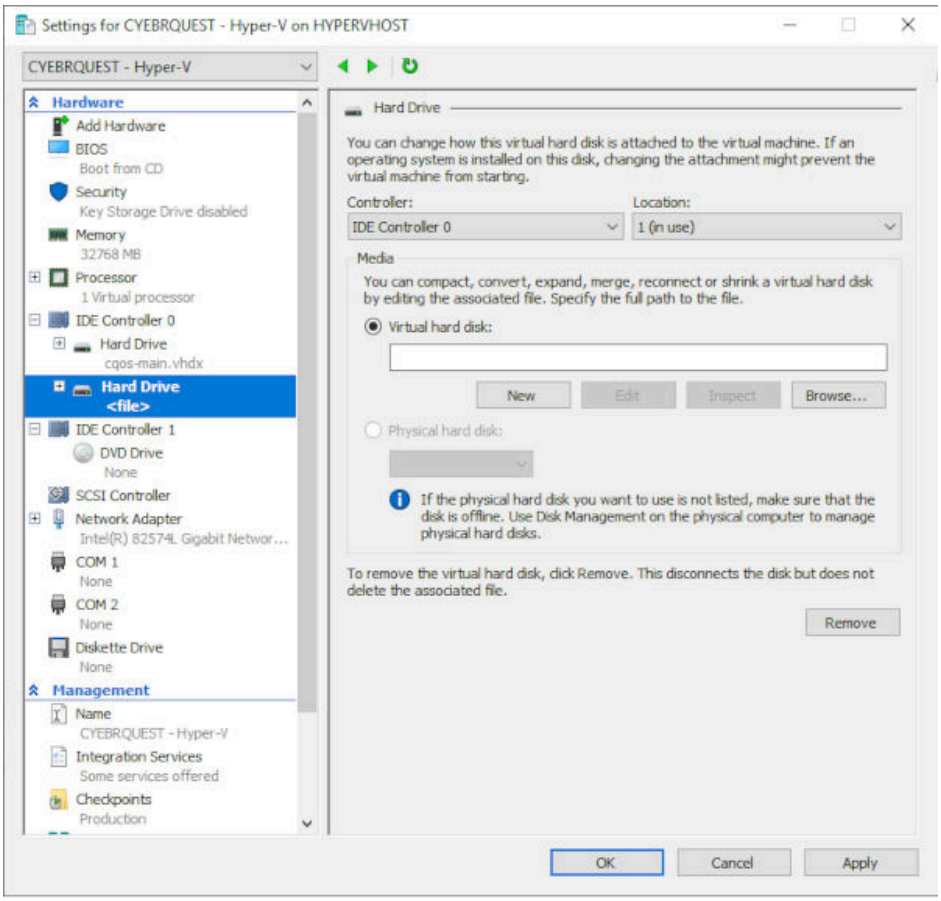




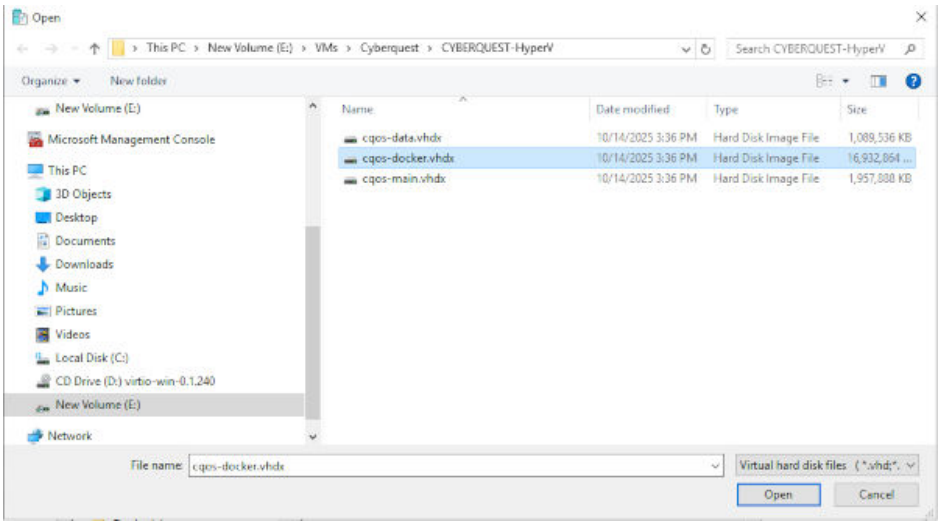
5.In the **Settings** window select **IDE Controller 0**. In the right side select **Hard Drive** option and click **Add**

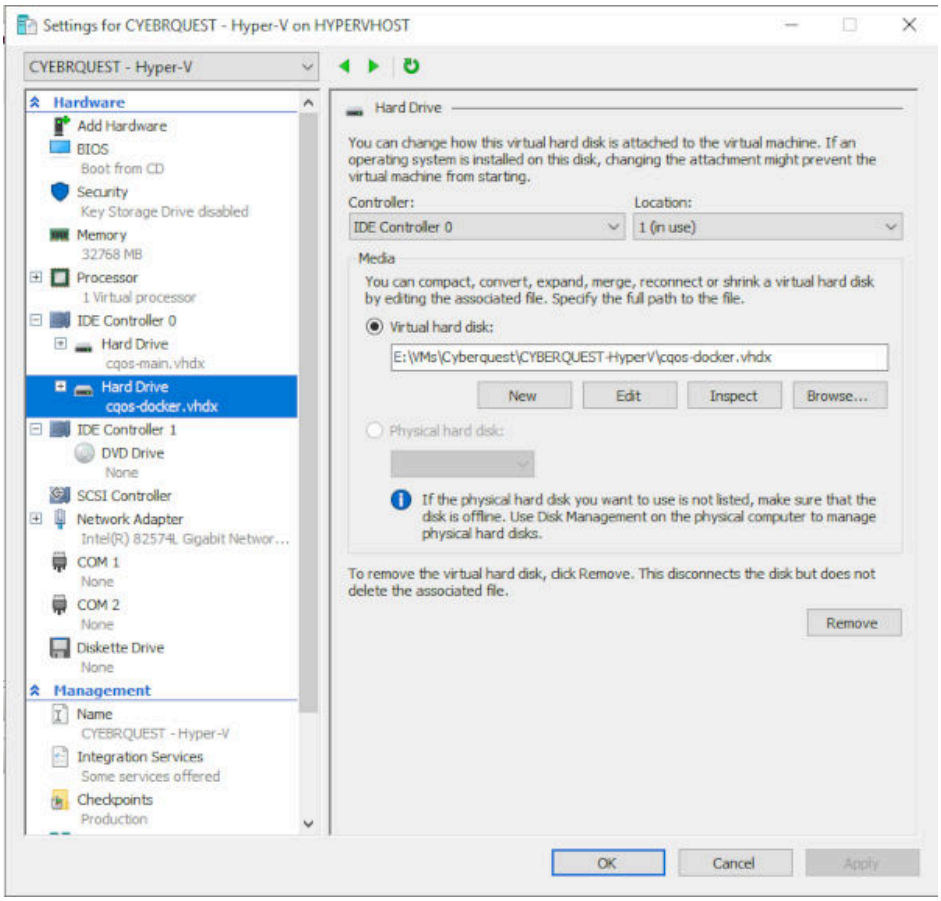


6.In the **Media** section, click **Browse** and navigate to the location where the CYBERQUEST server virtual hard disks are stored.

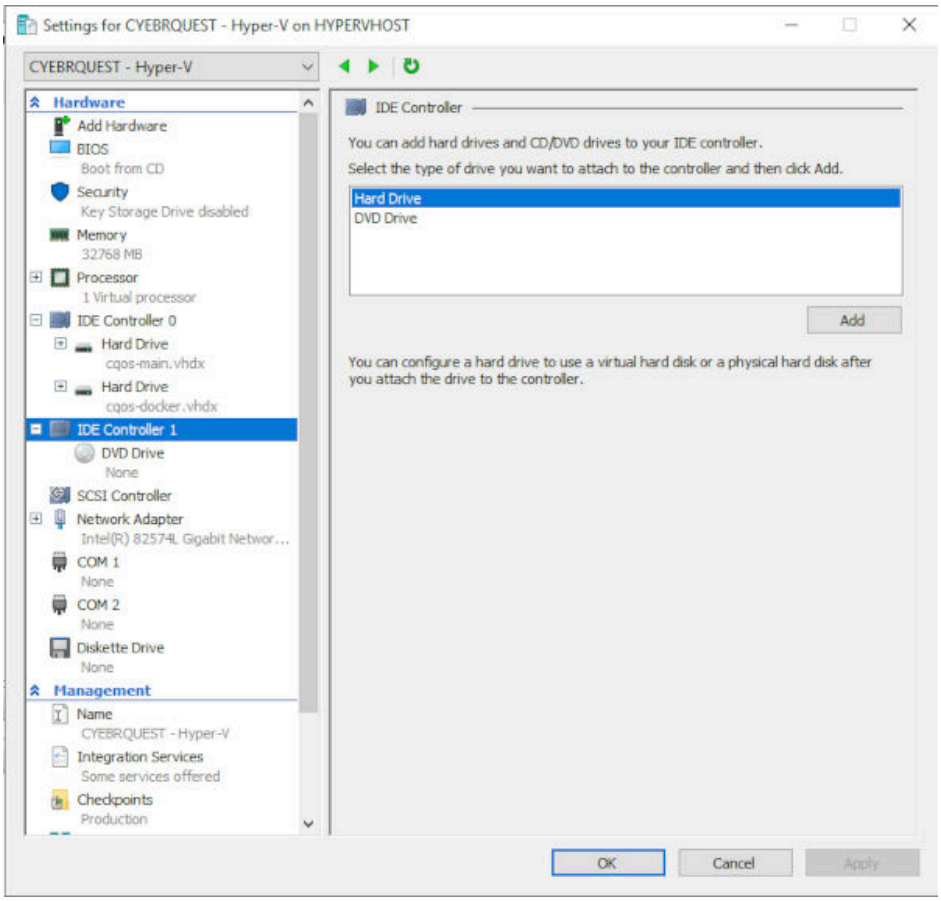


7.Select the **second disk file** *cqos-docker.vhdx*, and after click **Open** and **Apply**

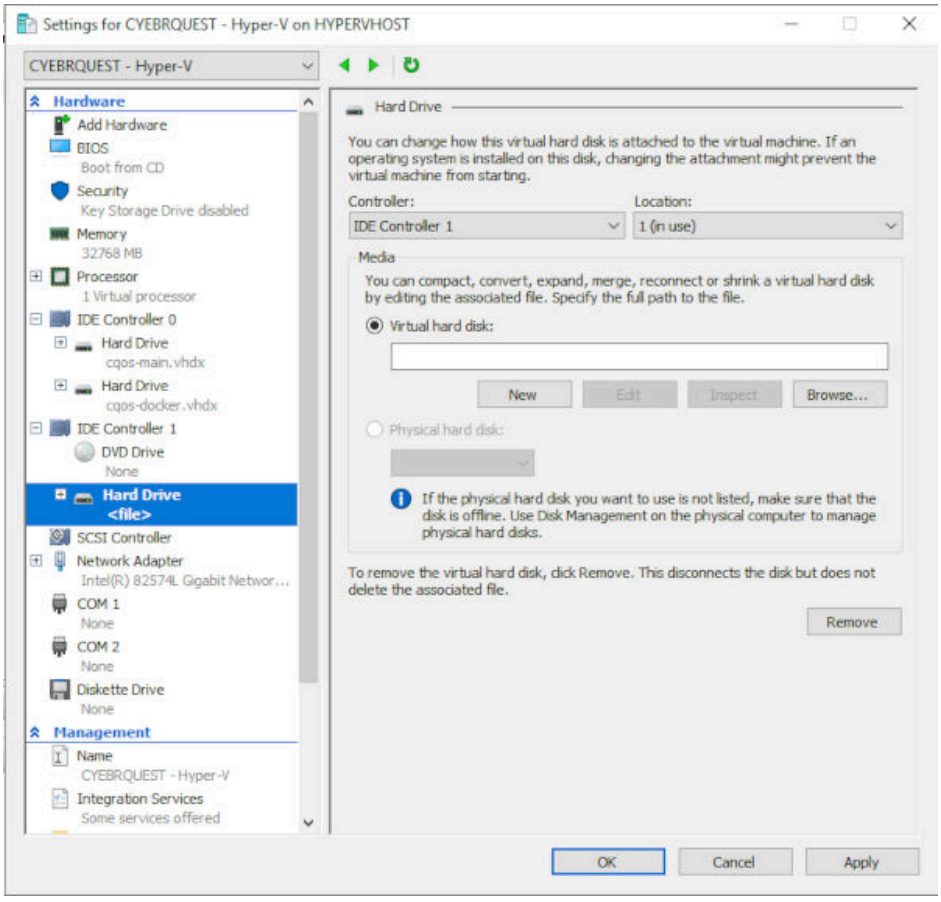




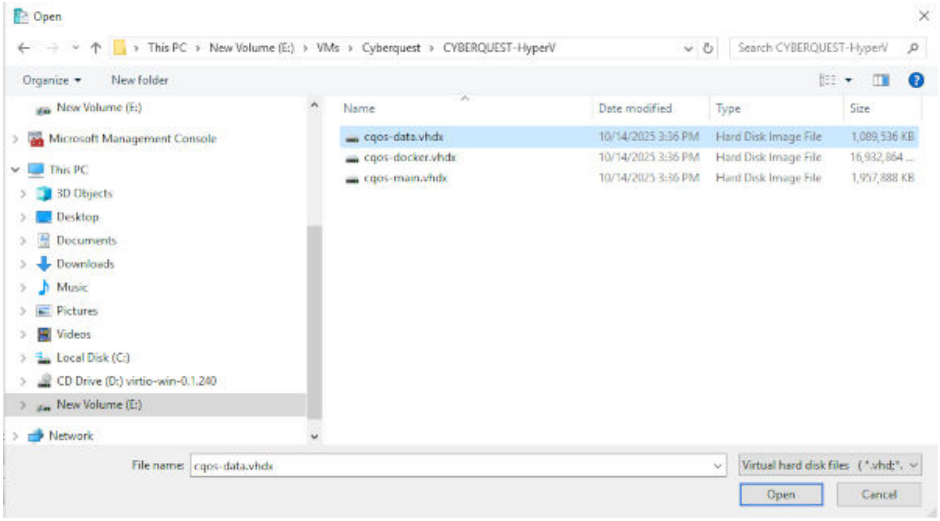
8.In the **Settings** window select **IDE Controller 1**. In the right side select **Hard Drive** option and click **Add**

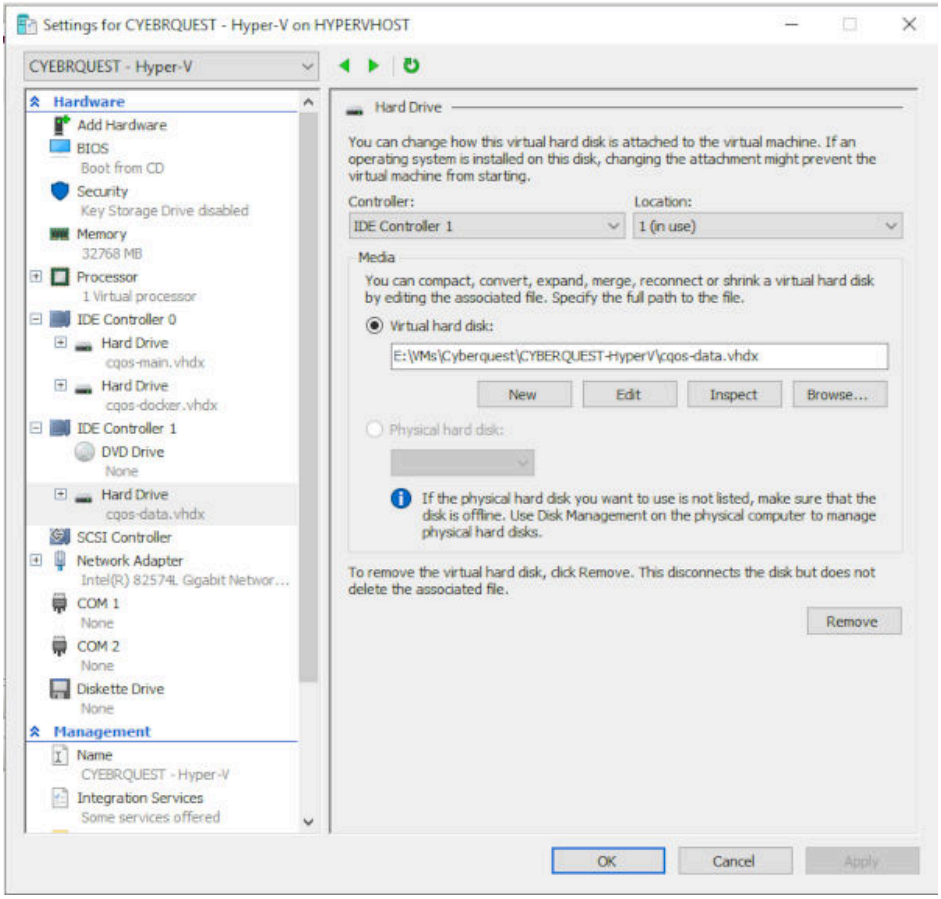


9.In the **Media** section, click **Browse** and navigate to the location where the CYBERQUEST server virtual hard disks are stored.

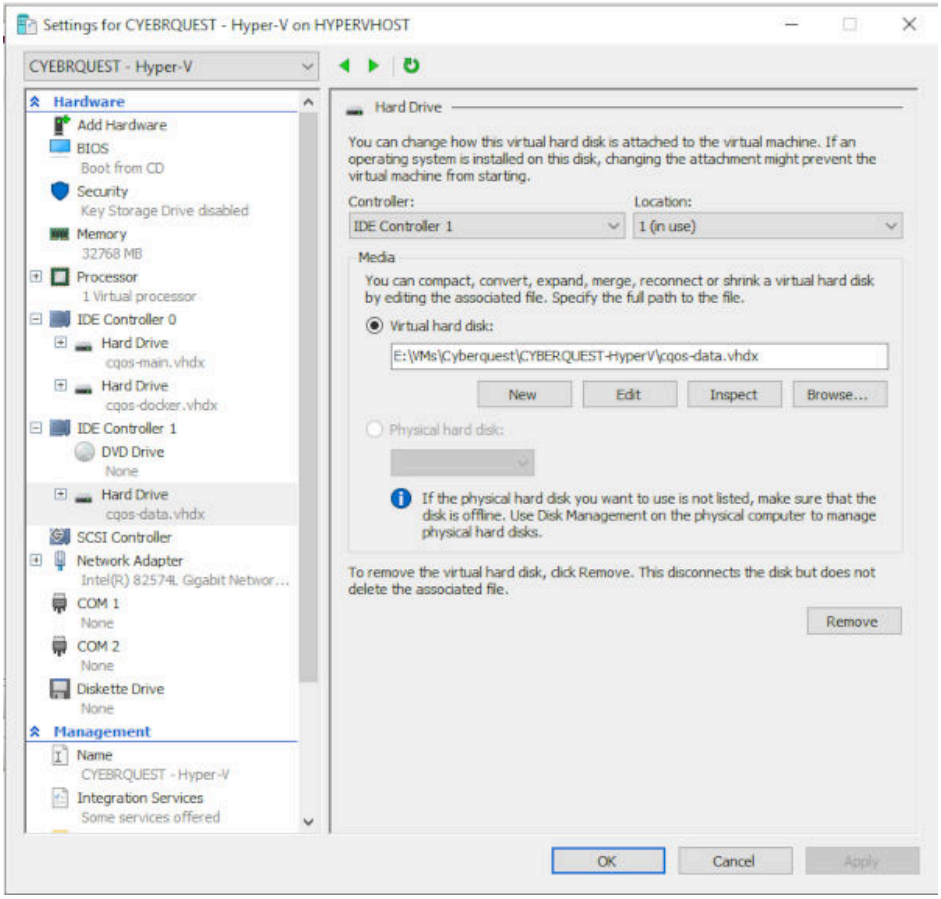


10.Select the **last disk file** *cqos-data.vhdx*, and after click **Open** and **Apply**





11.Click **OK** to complete adding the **CYBERQUEST Virtual Hard Disks**.



12.To set the TimeZone, use the following command and follow the interactive steps:

```
tzselect
```

```
superadmin@COOS2509:~$ tzselect
Please identify a location so that time zone rules can be set correctly.
Please select a continent, ocean, "coord", "TZ", "time", or "now".
1) Africa
2) Americas
3) Antarctica
4) Arctic Ocean
5) Asia
6) Atlantic Ocean
7) Australia
8) Europe
9) Indian Ocean
10) Pacific Ocean
11) coord - I want to use geographical coordinates.
12) TZ - I want to specify the timezone using a proleptic TZ string.
13) time - I know local time already.
14) now - Like "time", but configure only for timestamps from now on.
#? 8
```

```
Please select a country whose clocks agree with yours.
1) Åland Islands          8) Britain (UK)          15) Finland          22) Ireland          29) Luxembourg          36) Norway          43) Slovakia          50) Vatican City
2) Albania                9) Bulgaria              16) France           23) Isle of Man      30) Malta               37) Poland          44) Slovenia
3) Andorra               10) Croatia               17) Germany          24) Italy            31) Moldova             38) Portugal        45) Spain
4) Austria               11) Cyprus                18) Gibraltar        25) Jersey           32) Monaco              39) Romania         46) Sweden
5) Belarus               12) Czech Republic        19) Greece           26) Latvia           33) Montenegro          40) Russia          47) Switzerland
6) Belgium               13) Denmark               20) Guernsey         27) Liechtenstein    34) Netherlands         41) San Marino      48) Turkey
7) Bosnia & Herzegovina  14) Estonia               21) Hungary          28) Lithuania        35) North Macedonia     42) Serbia          49) Ukraine
#? 39
```

```
Based on the following information:

       Romania

TZ='Europe/Bucharest' will be used.
Selected time is now:   Thu Oct 16 10:36:07 EEST 2025.
Universal Time is now:  Thu Oct 16 07:36:07 UTC 2025.
Is the above information OK?
1) Yes
2) No
#? 1
```

13.The services start automatically. If they fail to start, log in as root, navigate to the *cyberquest-deployment* directory, and run the following command:

```
systemctl start cyberquest-deployment.service
```

To verify that the services have started, run the command:

```
docker ps -a
```

Agent Installation

Windows Agent

Manual deployment

How to manually deploy agent for Windows based collections

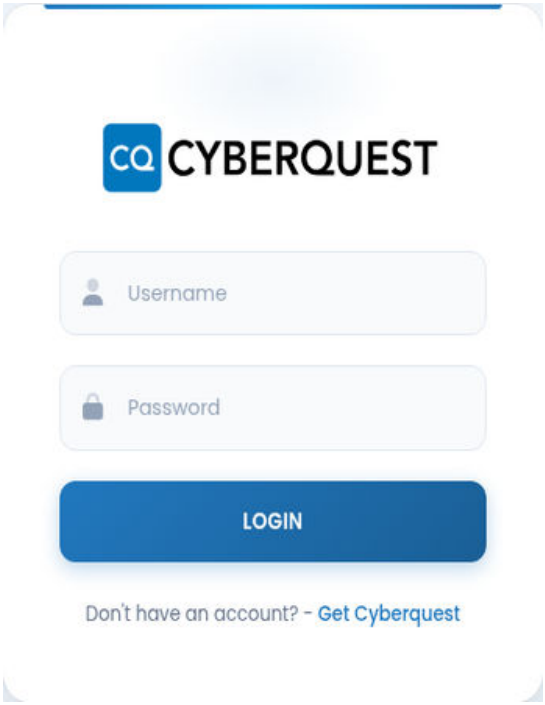
To install the CYBERQUEST agent on the Windows target machine, the following prerequisits must be met:

1. Install vcredist_x64_2010.exe (https://www.microsoft.com/en-us/download/confirmation.aspx?id=26999)
2. Install vcredist_x64_2012.exe (https://www.microsoft.com/en-us/download/confirmation.aspx?id=30679)
3. Install vc_redist_x64_2019.exe (https://aka.ms/vs/16/release/vc_redist.x64.exe)
4. Install Microsoft .NET Framework 4.8 (https://go.microsoft.com/fwlink/?linkid=2088631)

Authentication

To access Web Interface, open a web browser and type the application's address or DNS name. The default address initially assigned to Web Interface is ***https://CyberquestIPAddress*** (example).

The browser automatically redirects you to CYBERQUEST's authentication page:



How to manage Credentials

Creating the credentials set the agent is using for collecting data.

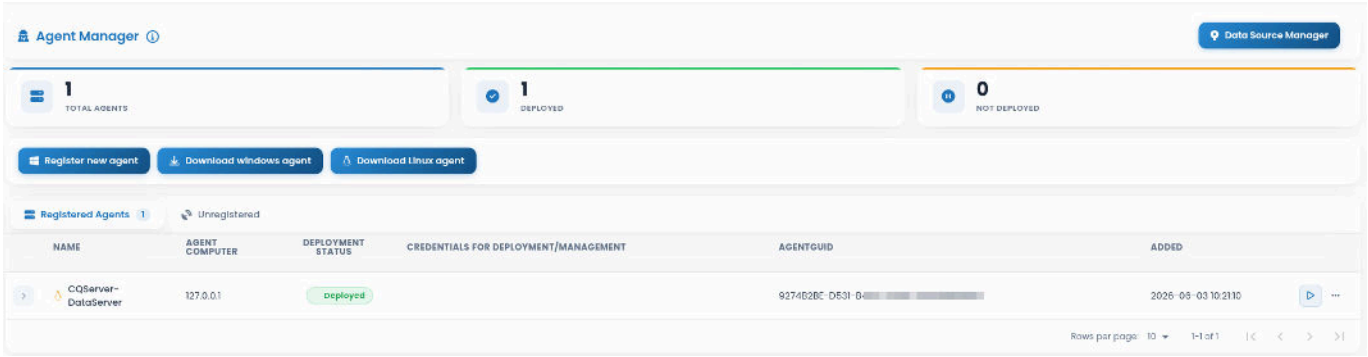
Please follow the link for more details.

Installing the CYBERQUEST agent

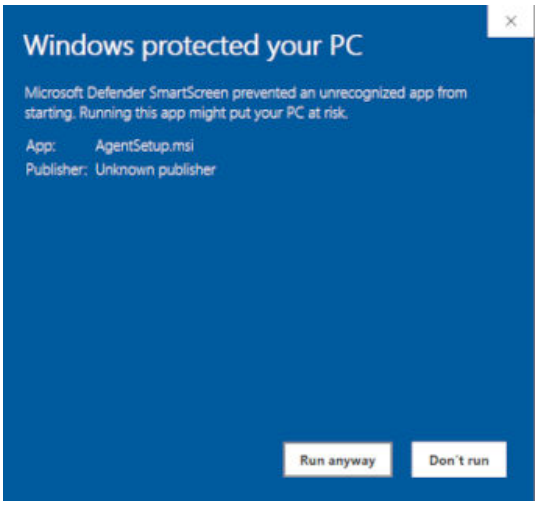
To manually deploy the agent, download or copy the agent kit on the target machine.

Navigate to **Settings** > **Management** > **Agent Manager**.

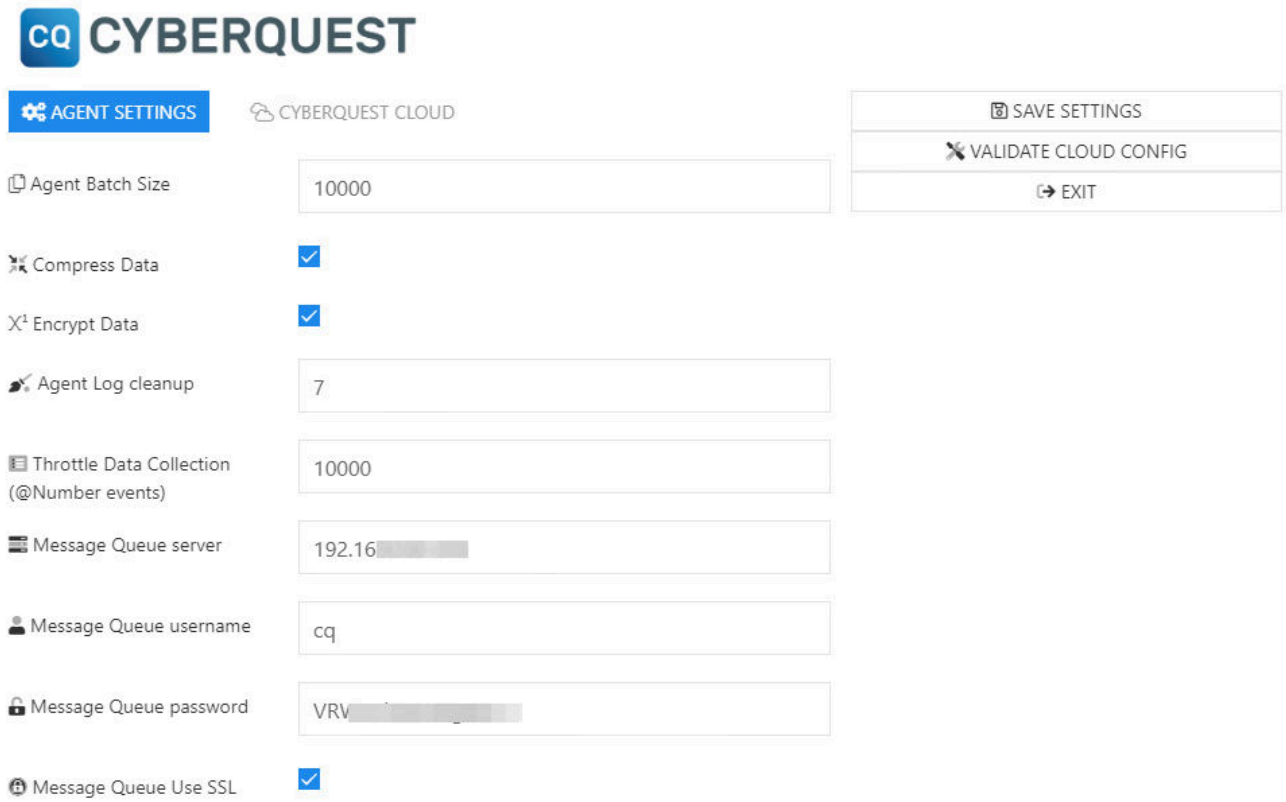
Click **"Download windows agent"** to download the latest version of the CYBERQUEST agent. The agent must be installed on a Windows machine.



Execute the .msi file and press the "Run anyway" button to install the agent. The agent is installed in: "C: \ Program Files \ CyberQuestAgent".



Go to "C:\Program Files\CyberQuestAgent\configurator" and run **cyberquest-agent-configurator.exe** as an Administrator. Add the IP address of the CYBERQUEST server in the field "Message Queue server" and press the "Save Settings" button.



Go to Windows services and restart the CYBERQUEST agent service.

Registering the agent

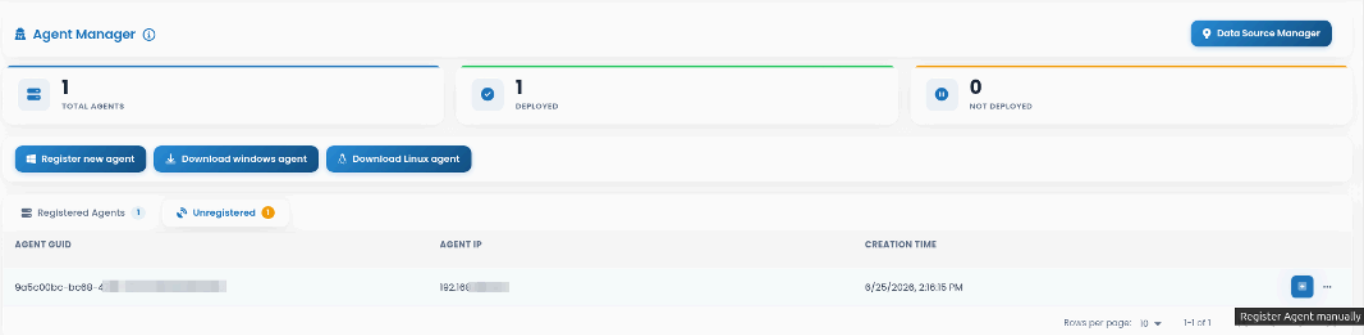
Registering the agent in the CYBERQUEST server:

Navigate to "**Settings** > **Management** > **Agent Manager**".

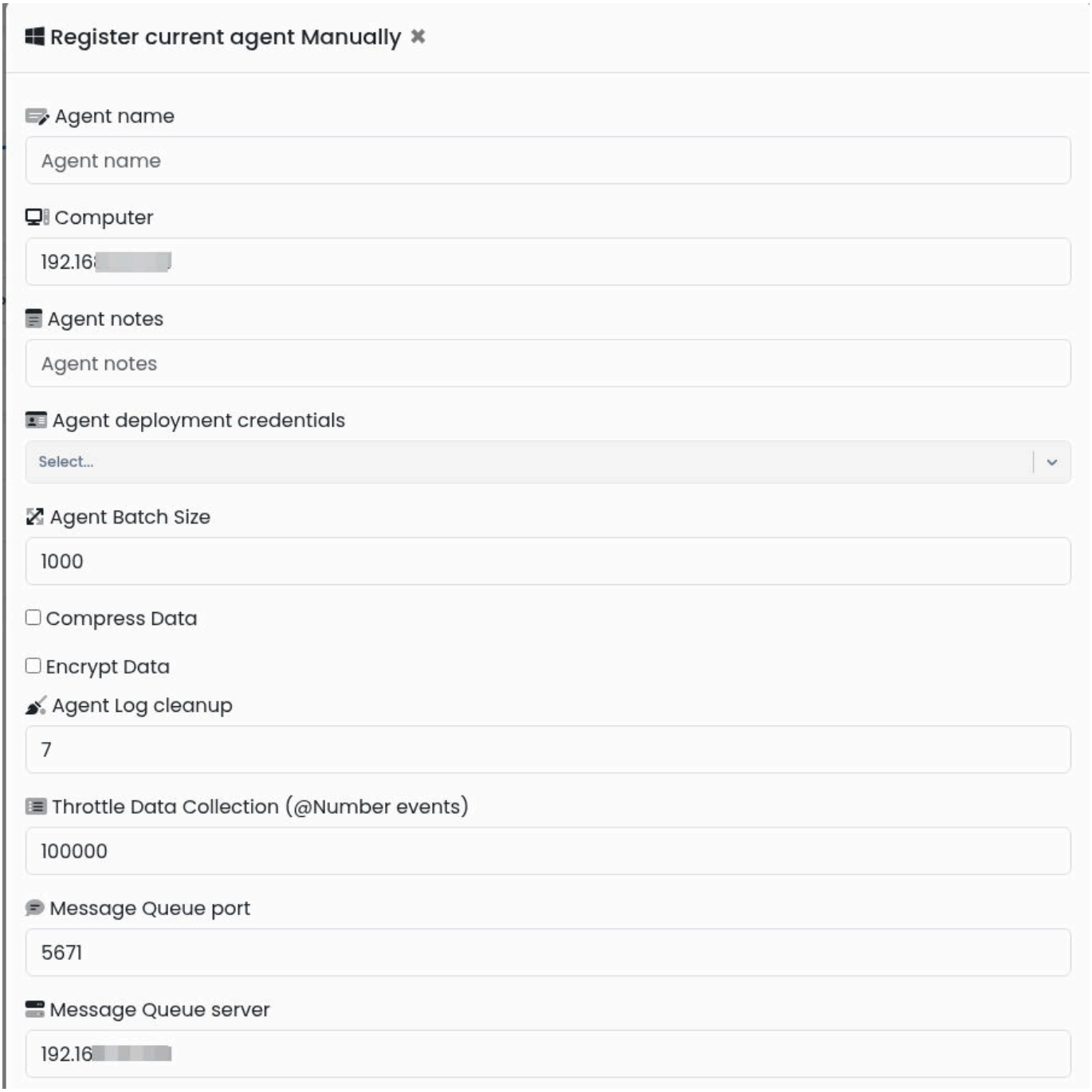
Go to ***Unregistered*** page and press

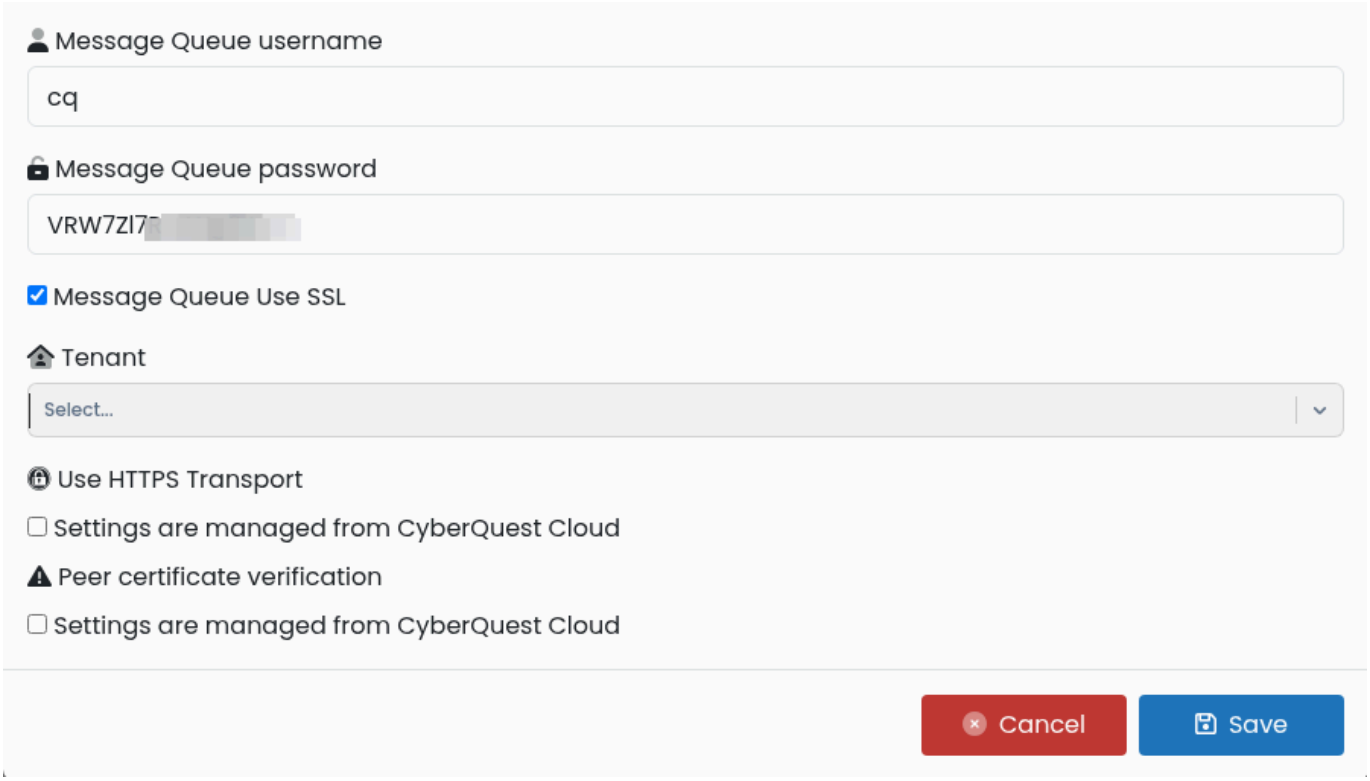


button to register the agent.



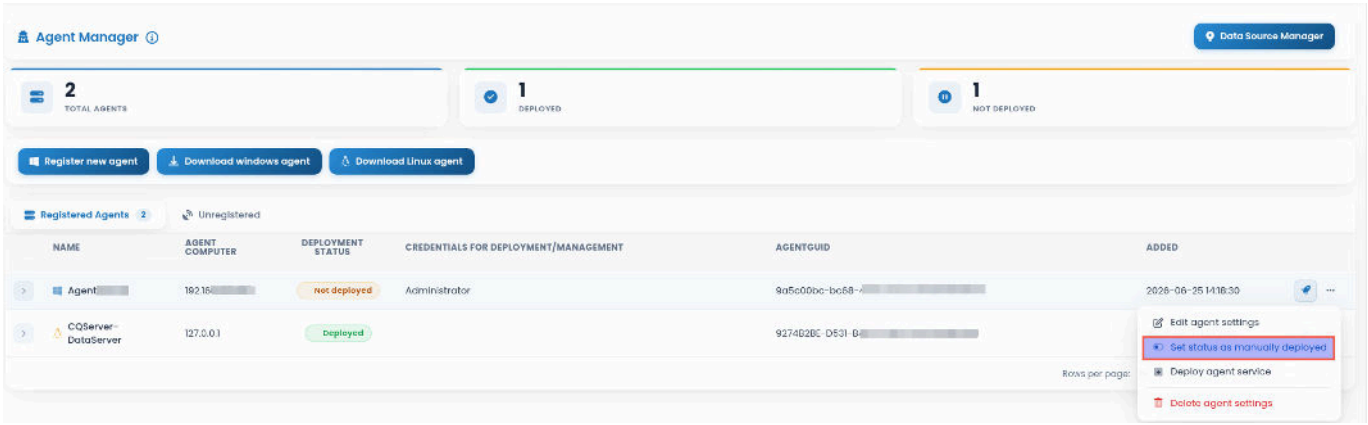
Complete the following fields: "Agent name", "Agent note", assign credentials for the agent and press "Save" button.


Register current agent Manually
Agent name
Agent name
Computer
192.16
Agent notes
Agent notes
Agent deployment credentials
Select...
Agent Batch Size
1000
Compress Data
Encrypt Data
Agent Log cleanup
7
Throttle Data Collection (@Number events)
100000
Message Queue port
5671
Message Queue server
192.16



After deployment, navigate to **Registered Agent** and click the **Set status as manually deployed**

button:



Adding a new data sources

The Windows agent is used to connect and collect Windows based data-sources like :

- WMI (Windows Management Instrumentation)
  - Windows Security Log
  - Windows Application Log
  - Windows System Log
  - Active Directory Information
- CQ Threat Intelligence
- ODBC Data Sources
- Oracle based DataSources

- MySQL (MariaDB) based DataSources
- API based data sources
- Text Files (freeText and CSV)

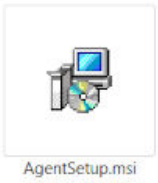
GPO deployment

Deploy CYEBERQUEST agent from GPO

To deploy CYBERQUEST Agent from GPO, please follow the steps described bellow:

1.Create a share accessible from all clients where the AgentCQ will be Deployed.

2.Copy the the following files:







3.Edit file **Copy config.ps1**

```
Copy-Item -Path \\FS_server\CQDeployShare\agent.settings.json -Destination "C:\Program Files\CyberQuestAgent"
Stop-Service -Name CyberQuestAgent
Start-Sleep -s 30
Start-Service -Name CyberQuestAgent
```

The path for the copyed files in step 2 is: **\FS_server\CQDeployShare**

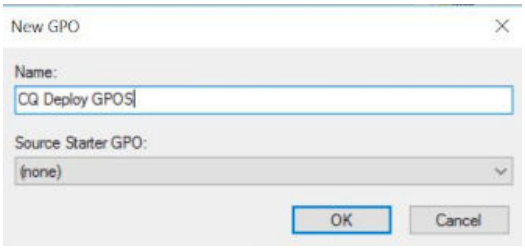
4.Edit **agent.settings.json** file

```
{
"mqPassword": "VRW7Zl7RreWg9Q==",
"eventSyncQueueSize": 5000,
"compressData": false,
"encryptData": false,
"cleanupOlderLogsDays": 7,
"throttleCollection": 1000000,
"mqHost": "0.0.0.0", //CYBERQUEST Server IP Address
"mqUserName": "cq",
"mqUseSSL": false,
"useHTTPSTransport": false,
"rejectUnauthorized": false,
"EventsThrottleQueueMaxSize": 100000,
"mqPort": 5672,
"mqSSLPort": 5671,
"tenant": "danielt-pc",
"HttpTransportUrl": "",
"CLIENT_ACCESS_TOKEN": ""
}
```

5.Go to Domain Controller and open **Group Policy Management**

6.Right click on the **Organization Unit** where the Policy will be applied (Ex: "Computers" OU) and select **Create a GPO in this domain, and Link it here**.

7.Name the new GPO **CQ Deploy GPO** and click **OK** button



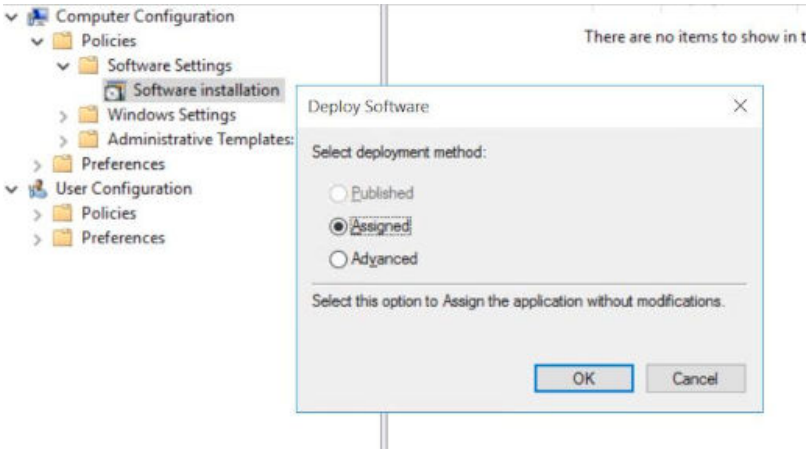
8.Right click on the new created GPO and select **Edit** option

9.Navigate to **Computer Configuration > Policies > Software Settings > Software Installation**

10.Right click on **Software Installation** and select **New > Package...**

11.Browse to the share location created in step 1 and configured in step 3 (\FS_server\CQDeployShare), select the MSI file and click **Open** button

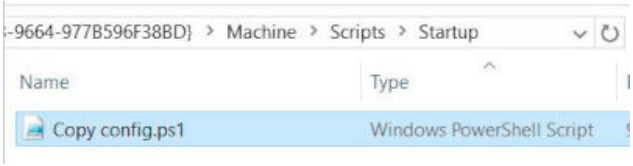
12.Select **Assigned** option and click **OK** button



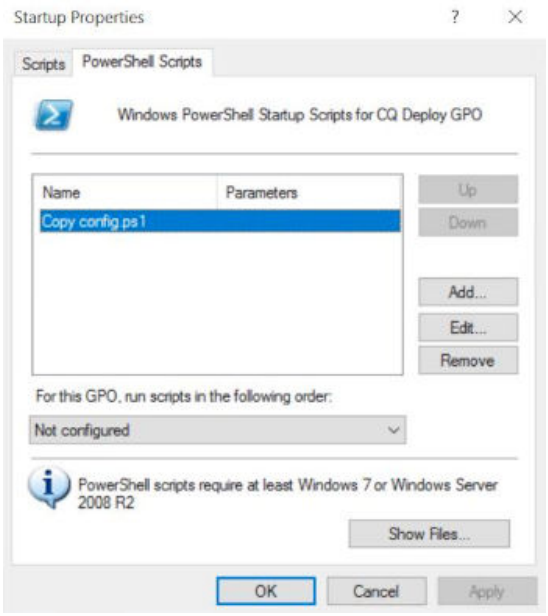
13.Navigate to **Computer Configuration > Policies > Windows Settings > Scripts (Startup/Shutdown)**, right click on **Startup** and select **Proprieties**

14.Go to **PowerShell Scripts** tab and press on **Show Files...** button

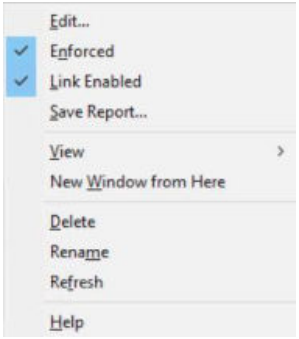
15.In the new File Explorer window copy the PowerShell script file (Copy config.ps1) from the shared folder created on step 1



16.Click on **Add...** button, click on **Browse** button, select the PowerShell Script **Copy config.ps1** and click **Open** and then **OK** > **Apply** > **OK**



17.Close **Group Policy Management Editor**, right click on the new GPO and select **Enforced** option



Remote installation

To install the CYBERQUEST agent on the Windows target machine, the following prerequisits must be met:

1. Install vcredist_x64_2010.exe (https://www.microsoft.com/en-us/download/confirmation.aspx?id=26999)
2. Install vcredist_x64_2012.exe (https://www.microsoft.com/en-us/download/confirmation.aspx?id=30679)
3. Install vc_redist_x64_2019.exe (https://aka.ms/vs/16/release/vc_redist.x64.exe)
4. Install Microsoft .NET Framework 4.8 (https://go.microsoft.com/fwlink/?linkid=2088631)

To start, first configure the deploy credentials. Please follow the link for more details about creating credentials.

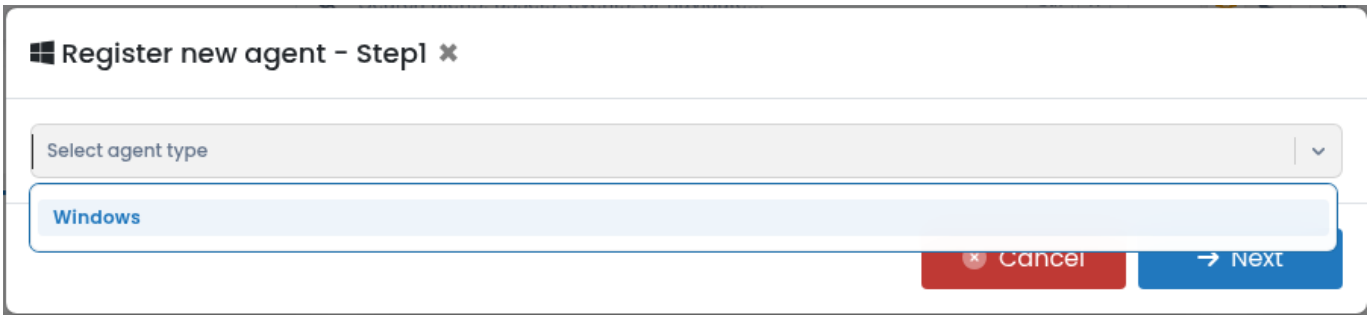
**Deploying CYBERQUEST agent on Windows **

The next step is to deploy the CYBERQUEST agent on Windows operating system, by clicking on **Settings > Management > Agent Manager**, and click on

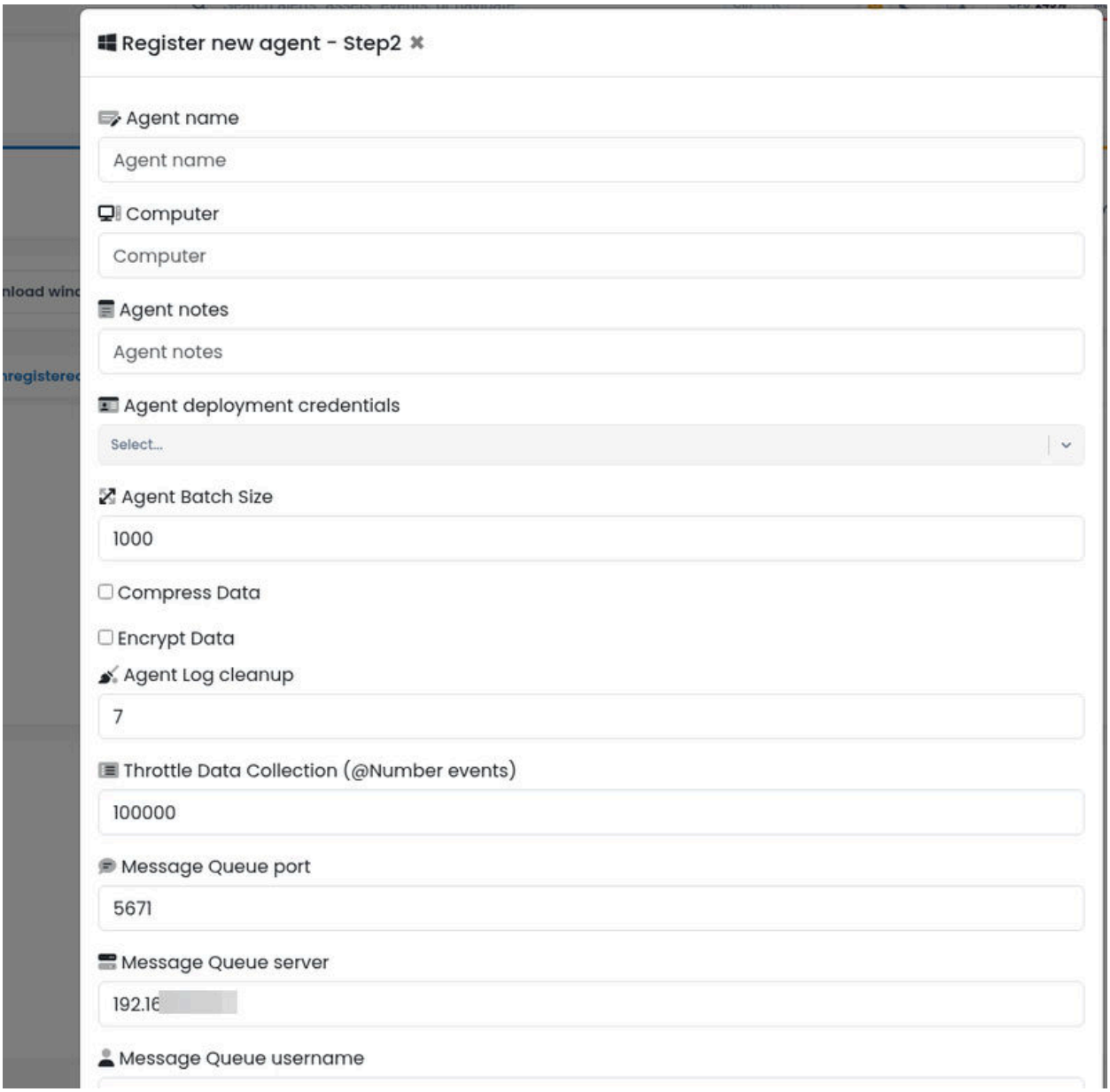


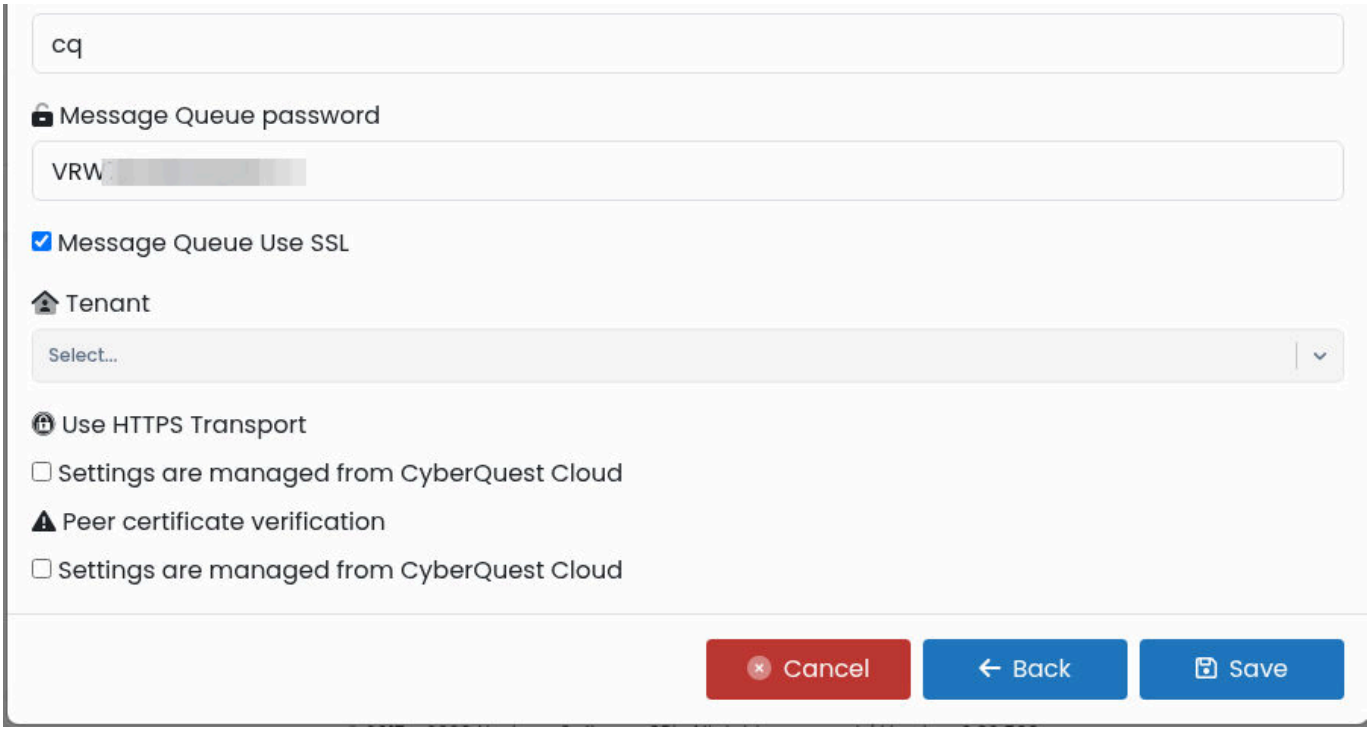
button.

To register a new agent, the user will first be asked the operating system on which to deploy the agent, with the option of Windows.



Once selected, the settings of the agent deployment will be filled in. Complete the following fields: "Agent name", "Computer", select "Agent deployment credentials" and press "Save" button.





Lastly, data sources can be linked to the CYBERQUEST agent.

The Windows agent is used to connect and collect Windows based data-sources like :

- WMI (Windows Management Instrumentation)
  - Windows Security Log
  - Windows Application Log
  - Windows System Log
  - Active Directory Information
- CQ Threat Intelligence
- ODBC Data Sources
- Oracle based DataSources
- MySQL (MariaDB) based DataSources
- API based data sources
- Text Files (freeText and CSV)

Managing Windows Gathering Agent
Manage CYBERQUEST Log Gathering configuration files

For more details about manually deploy Agent and assign data sources, please access the following link: How to manually deploy agent and assign data sources

Please note that in order to successfully change entries in configuration files, the agent service must be in stopped state:

a. Using an administrative account, authenticate to the Windows log gathering computer having the agent installed and open **Services management console**

b. **Stop** CYBERQUEST Log Gathering Agent service.

c. After finished performing changes, **start** CYBERQUEST Log Gathering Agent service.

To see how to manually deploy the agent, please follow the link: How to manually deploy the agent

CYBERQUEST One-Click Installation for other Operating Systems

One-Click Install has been tested and validated on the following operating systems:

- *Debian 12*
- *Debian 13*
- *RedHat 9.4*
- *RedHat 9.6*
- *RedHat 10.0*
- *Ubuntu 22.04*
- *Ubuntu 24.04 LTS*

The following prerequisites are required on all supported operating systems before starting the deployment:

- **sudo** (user must be in the sudoers list) and **root** privileges
- **curl**
- **Docker**

Prior installation system requirements

In order to configure the virtual machine, the following requirements must be met first:

- Three partitions:
  - minimum 34 GB (where the Operating System will be installed)
  - minimum 32 GB (where the Docker containers are stored)
  - minimum 10 GB (where the data will be stored)

  If these partitions contain any data, the existing data will be deleted during the installation process.
- An internet connection is required;
- 4 CPU cores;
- Minimum 32 GB RAM.

CYBERQUEST Deployment on Ubuntu 24.04 VMs

Implementing a CYBERQUEST virtual environment requires precise configuration to ensure proper operation and consistency across systems. This guide provides a simplified approach to configuring CYBERQUEST on virtual machines, reducing setup time and minimizing potential configuration errors.

The steps in this guide apply to all supported operating systems. Only on Red Hat-based systems are additional commands required.

The steps below detail the deployment of CYBERQUEST on **Ubuntu 24.04**, including environment setup and configuration:

Step 1: Run the following command as **root** to start the CYBERQUEST deployment.

```
mkdir cyberquest-deployment && cd cyberquest-deployment &&  curl -O https://download.cyberquest.cloud/install_sfx.sh
&& sudo bash ./install_sfx.sh
```

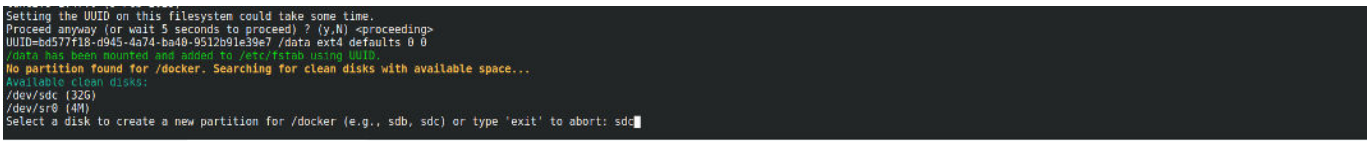
Step 2: After executing the installation script, a prompt will appear asking **"Do you want to proceed with the application installation?"**. Select **y** and press **ENTER** to move forward with the deployment.



Step 3: Once Docker is installed, the script will check for available disks to create a partition for **/data**. A list of clean disks will be displayed. Select a disk (e.g., `sdb` or `sdc` and press **ENTER**) to create the new partition.



Step 4: The deployment script mounts the **/data** partition and updates `/etc/fstab` to ensure it is automatically mounted on boot. It then scans for available disks to create a partition for **/docker**. Choose a disk from the list to allocate space for Docker storage and continue the deployment.



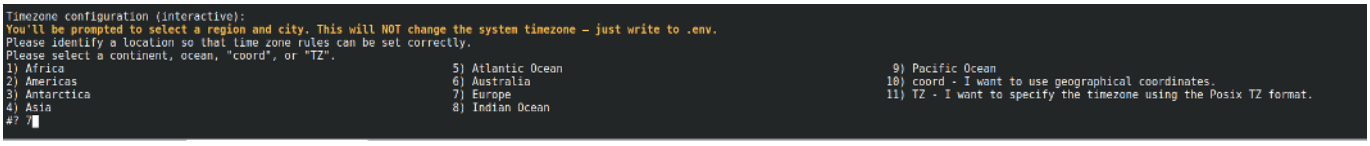
Step 5: After the preparation script completes, the TLS configuration is initialized. By default, only **TLS 1.3** is enabled.



note that TLS 1.3 requires Windows 11 or newer, or Windows Server 2019 or newer for the agent collector.

When prompted, choose whether to also enable **TLS 1.2** by typing `y` for yes or `n` for no.

Step 6: Set the timezone for CYBERQUEST by selecting the appropriate region and city. This ensures that time-related settings in the application are configured correctly.



Step 7: Select the country that matches the local time. This helps CYBERQUEST apply the correct time settings for the environment.



Step 8: Review the timezone information that was set based on the previous selections. Confirm that the displayed local and universal times are correct by choosing **Yes** to proceed or **No** to make adjustments.

```
The following information has been given:

        Romania

Therefore TZ='Europe/Bucharest' will be used.
Selected time is now:    Thu Oct 16 11:59:57 EEST 2025.
Universal Time is now:   Thu Oct 16 08:59:57 UTC 2025.
Is the above information OK?
1) Yes
2) No
#? 1
```

Step 9: Configure the Java heap size, which determines the amount of memory allocated to the Java Virtual Machine for CYBERQUEST. Enter the size in GB or press Enter to use the default value.

```
Java heap size configuration:
Enter heap size in GB (default: 7):
```

Step 10: In the `cyberquest-deployment` directory, run the following command to download the latest CYBERQUEST Docker images:

```
docker compose pull
```

⚠️ Attention - RedHat Only

For RedHat systems, the following commands must be executed **before starting the CYBERQUEST services** to allow HTTPS access through the firewall:

```
sudo firewall-cmd --zone=public --add-service=https --permanent
sudo firewall-cmd --reload
```

```
sudo firewall-cmd --reload
```

Step 11: Start the CYBERQUEST deployment service by running the following command:

```
docker compose up -d
```

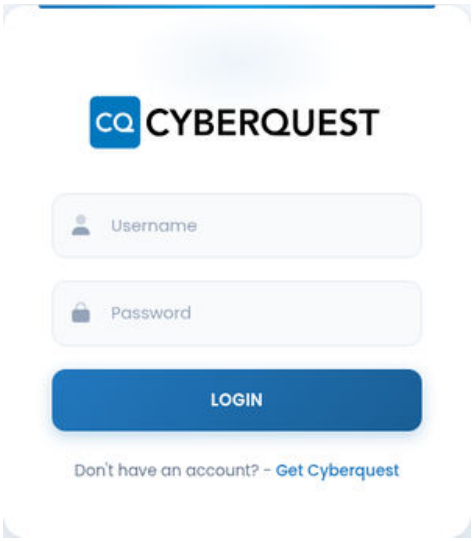
Step 12: Check the status of the CYBERQUEST services to verify they are starting correctly by running:

```
docker ps -a
```

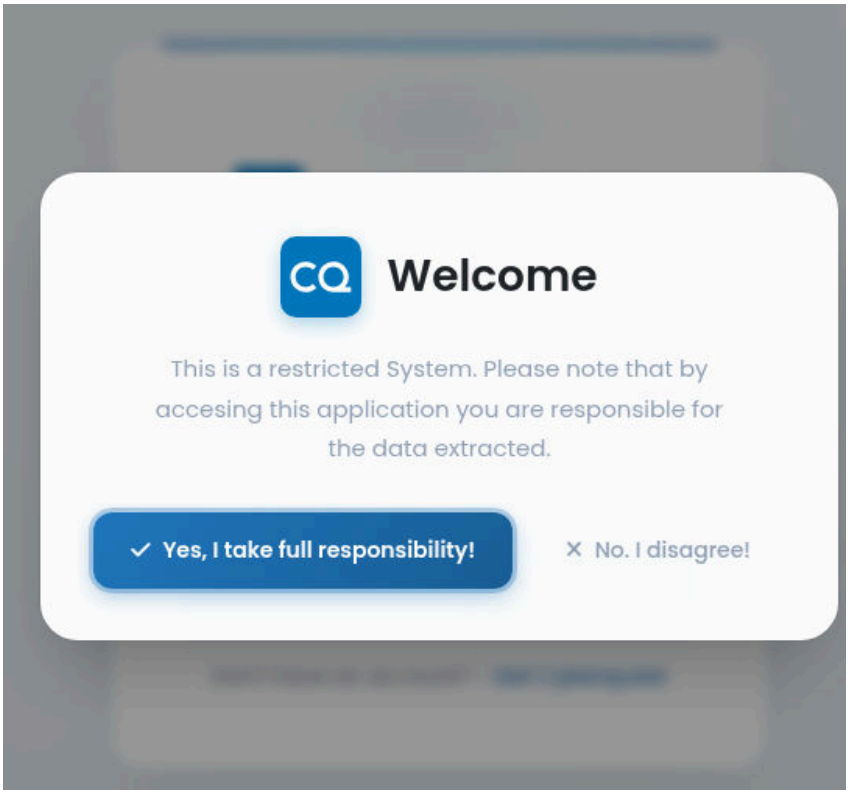
To log in to the CYBERQUEST application, enter the default username and password, then choose the desired interface language.

Default Username: superadmin

Default Password: toor1



You will be prompted with a default message about accessing restricted information. This message is fully customizable.

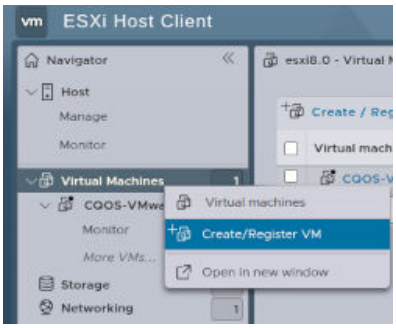


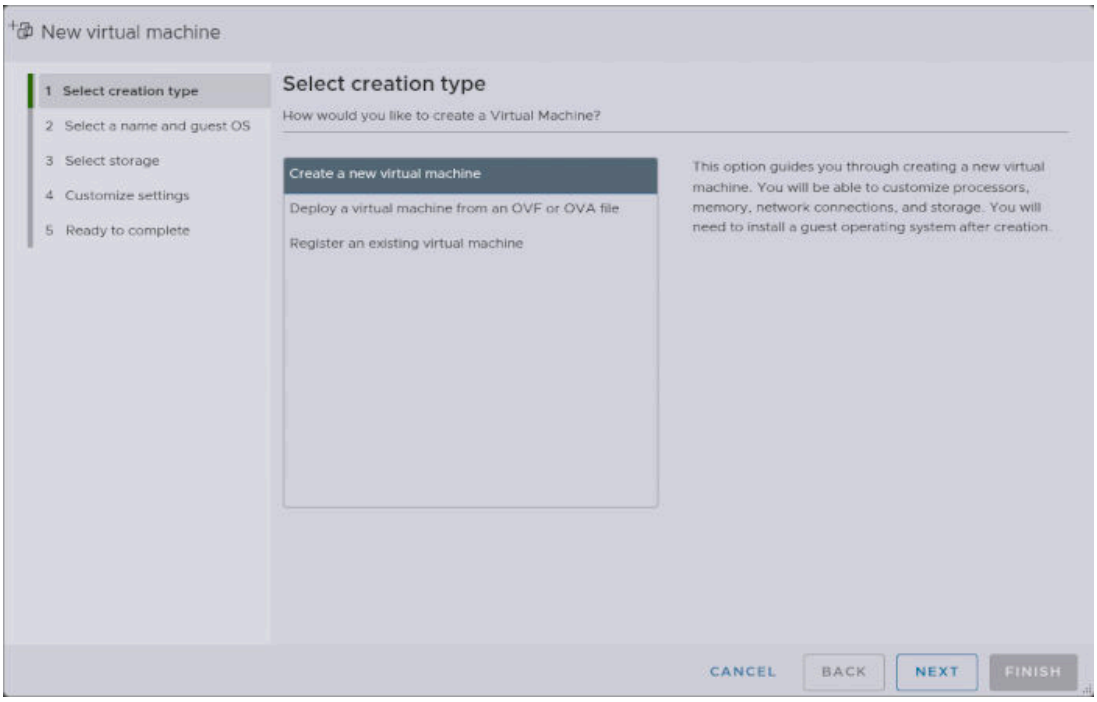
Accept the responsibility by clicking the button "***Yes, I take full responsibility!***". Else "***No. I disagree!***" and you will be redirected to the authentication page.

How to install Ubuntu 24.04 LTS on VMware

1.Download the Ubuntu 24.04 LTS ISO from the official Ubuntu site [Ubuntu 24.04 (https://ubuntu.com/download/desktop/thank-you?version=24.04.3&architecture=amd64&lts=true)](https://ubuntu.com/download/desktop/thank-you?version=24.04.3&architecture=amd64&lts=true).

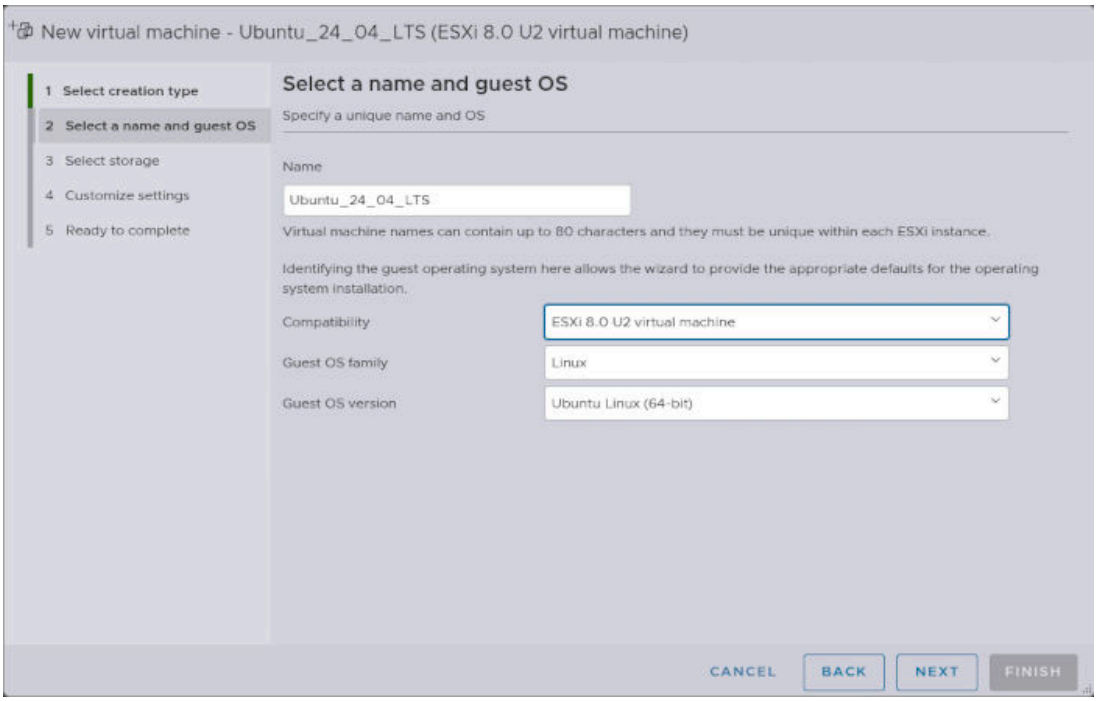
2.Open VMware Workstation/Player > Create/Register VM > Create a new virtual machine.



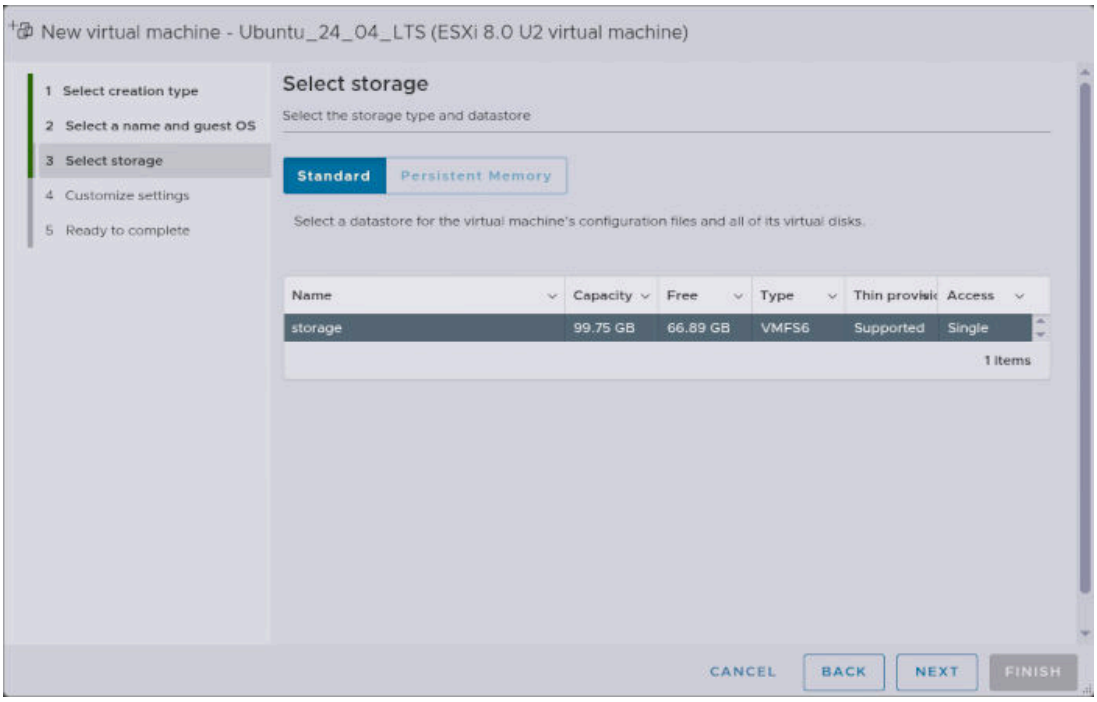


3.Choose guest OS type:

- Name: Ubuntu_24_04_LTS
- Compatibility: ESXi 8.0 U2 virtual machine
- Guest OS family: Linux
- Guest OS version: Ubutu Linux (64-bit)



4.Select storage: Select a datastore for the virtual machine's configuration files and all of its virtual disks.



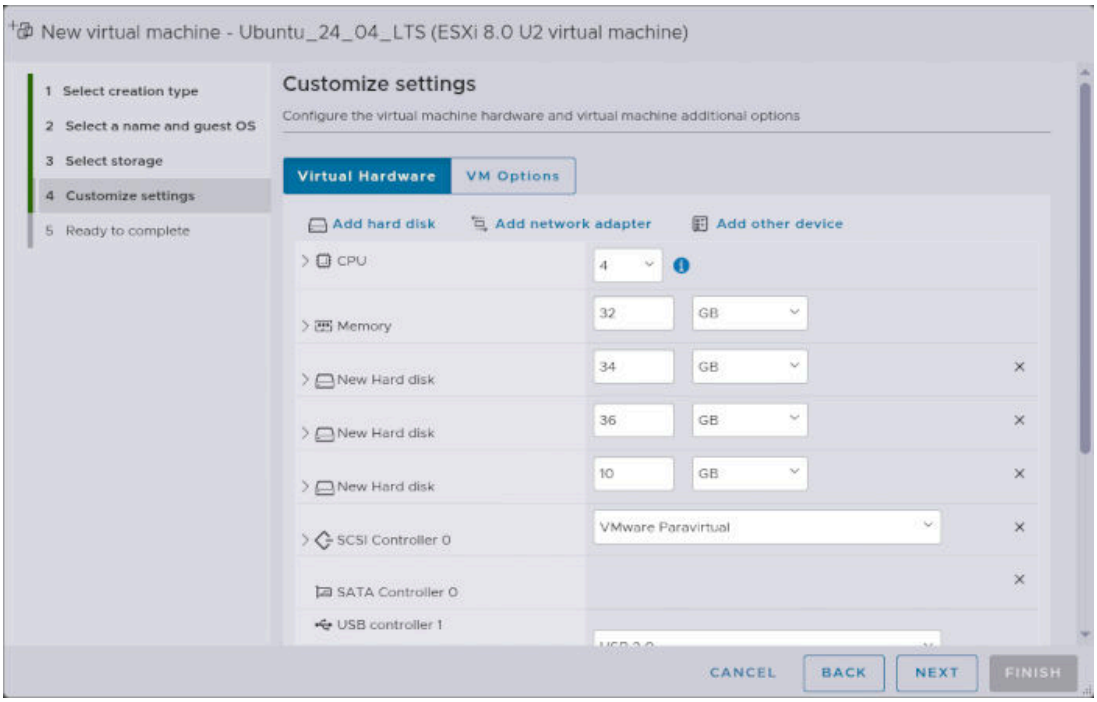
5.Customize settings - configure the virtual machine hardware and additional options.

Configure “CPU” and “Memory” according to your needs.

- The recommendation is a minimum of 4 cores.
- The recommendation for the Memory is a minimum 32048 MiB.

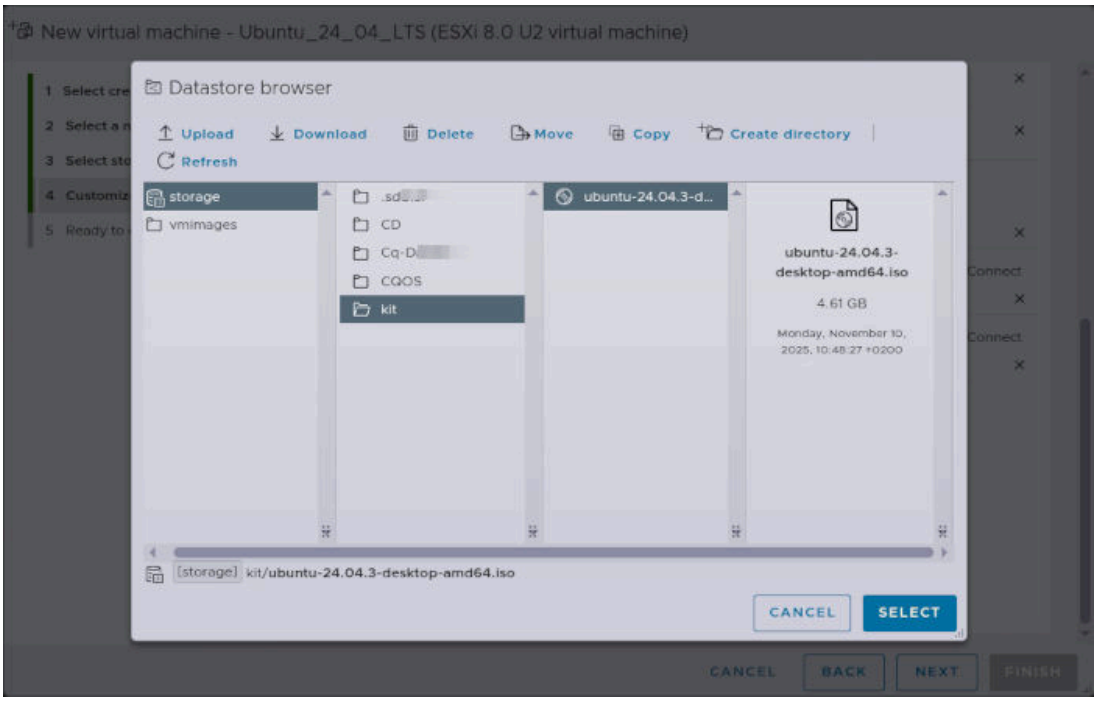
Configure three disk partitions. To add more disk partitions click on **Add hard disk** and choose **New standard hard disk**.

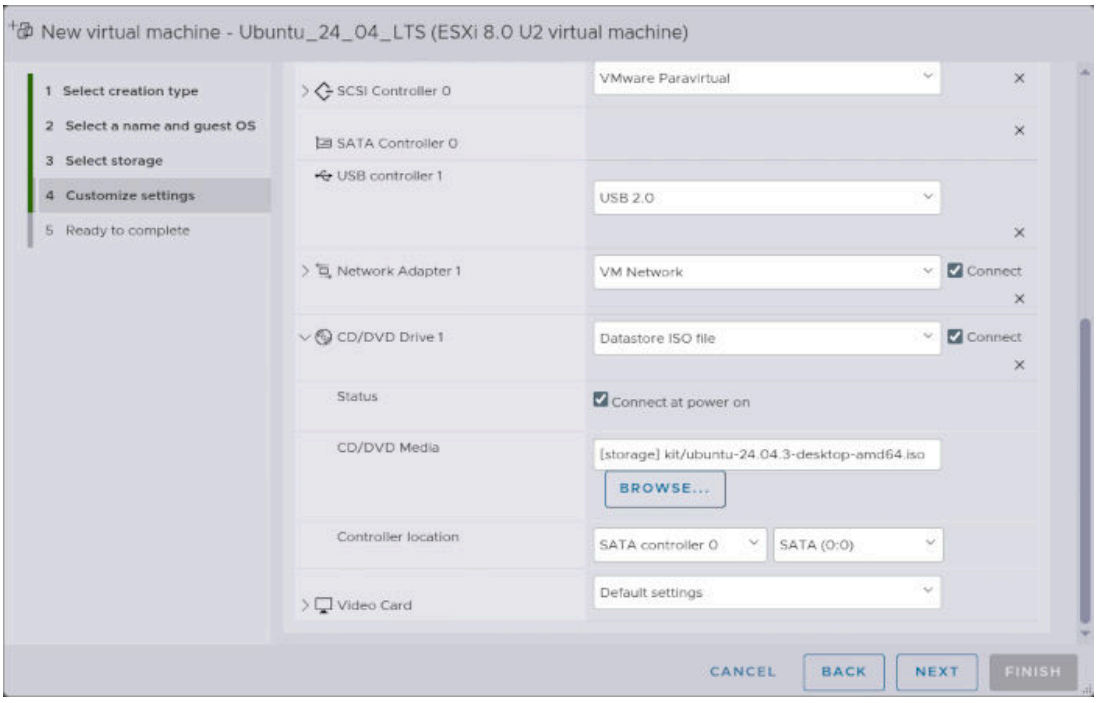
- Hard disk 1 - 10 GB (where the Operating System will be installed)
- New Hard disk - 32 GB (where the Docker containers are stored)
- New Hard disk - 10 GB (where the data will be stored)



Configure “Network” settings.

Go to **CD/DVD Drive 1** choosing **Datastore ISO file** and select the ubuntu-24.04.3-desktop-amd64.iso.



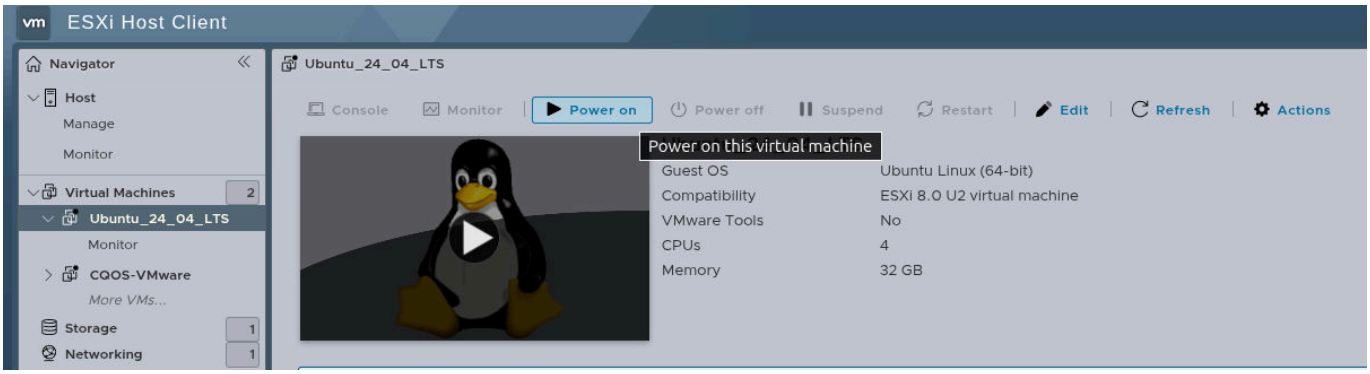


6.Review and confirm the settings.

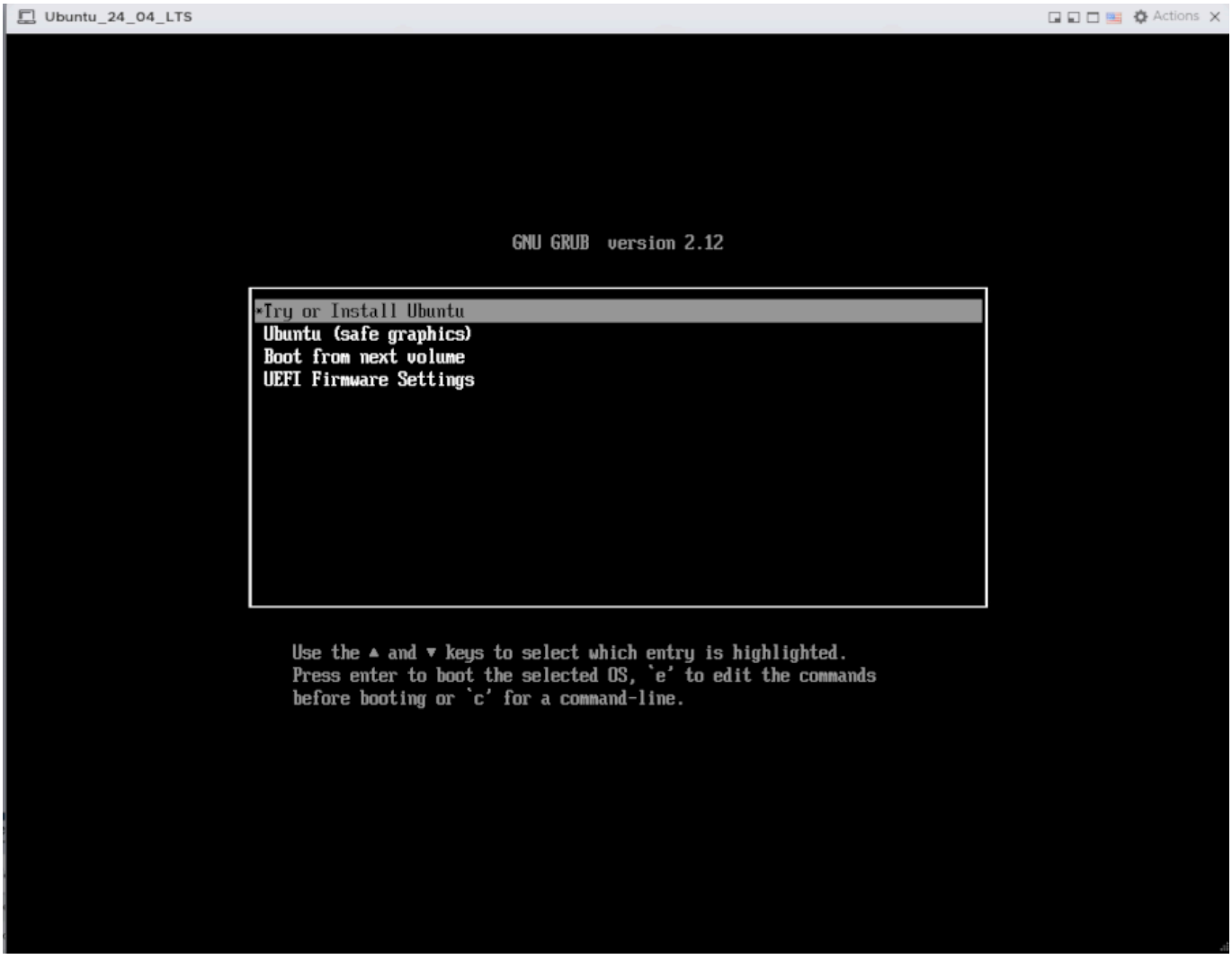
Ubuntu 24.04 Installation

1.Boot the VM

Start the virtual machine in VMware to begin the Ubuntu installation process. Ensure the Ubuntu ISO is mounted so the VM can boot from it.

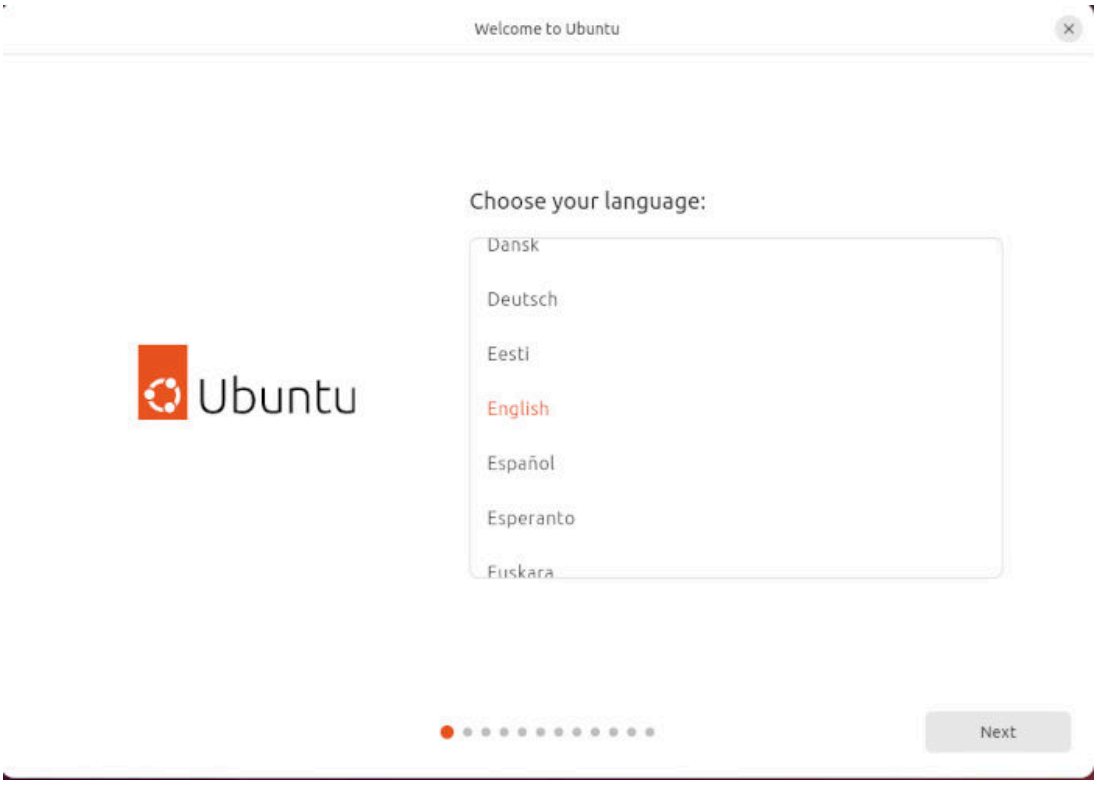


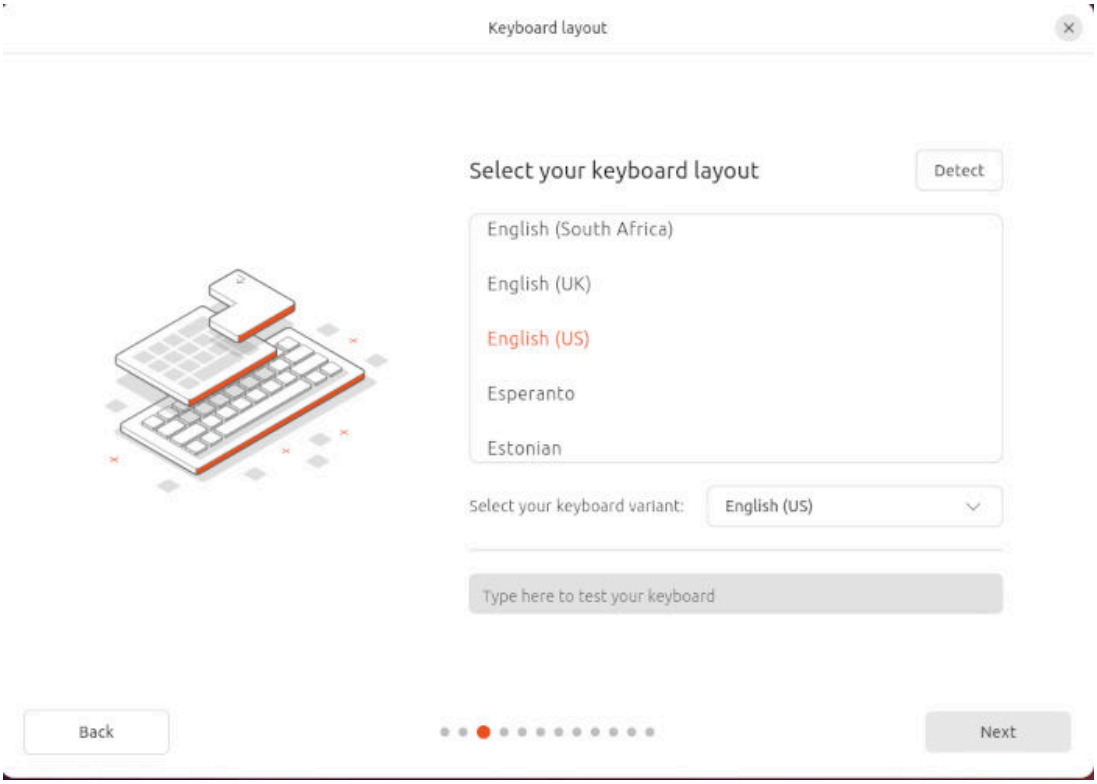
The VM will boot from the ISO file `ubuntu-24.04.3-desktop-amd64.iso`. When the boot menu appears, select **Install Ubuntu** to begin the installation process.



2.Select Language and Keyboard

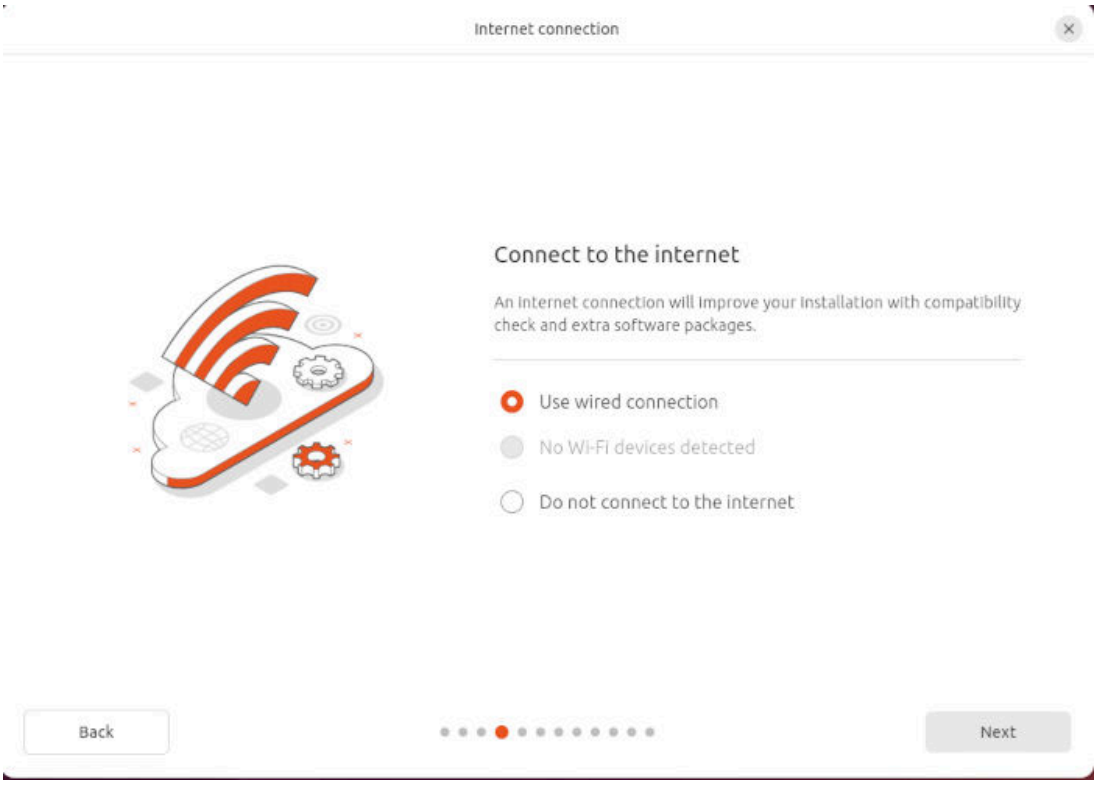
Choose the preferred language for the system interface and the desired keyboard layout for input.





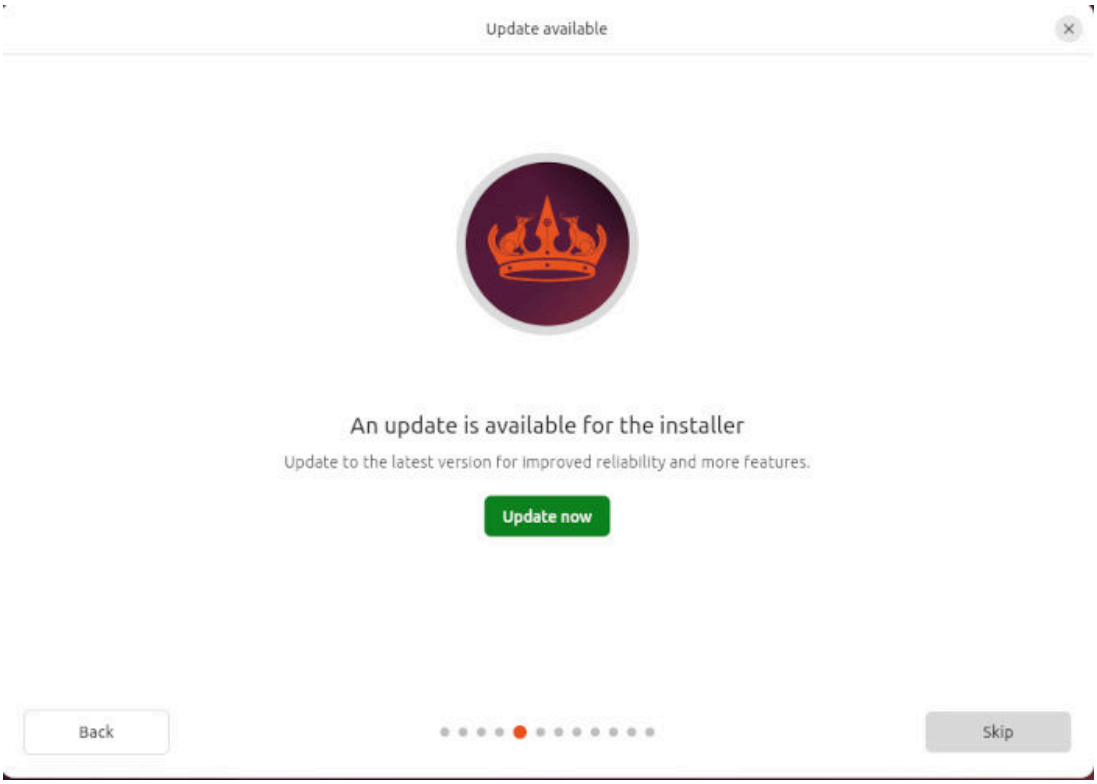
3.Connect to the internet

Ensure the VM is connected to a network. Select the available Wi-Fi or wired connection to enable downloading updates and third-party software during installation.



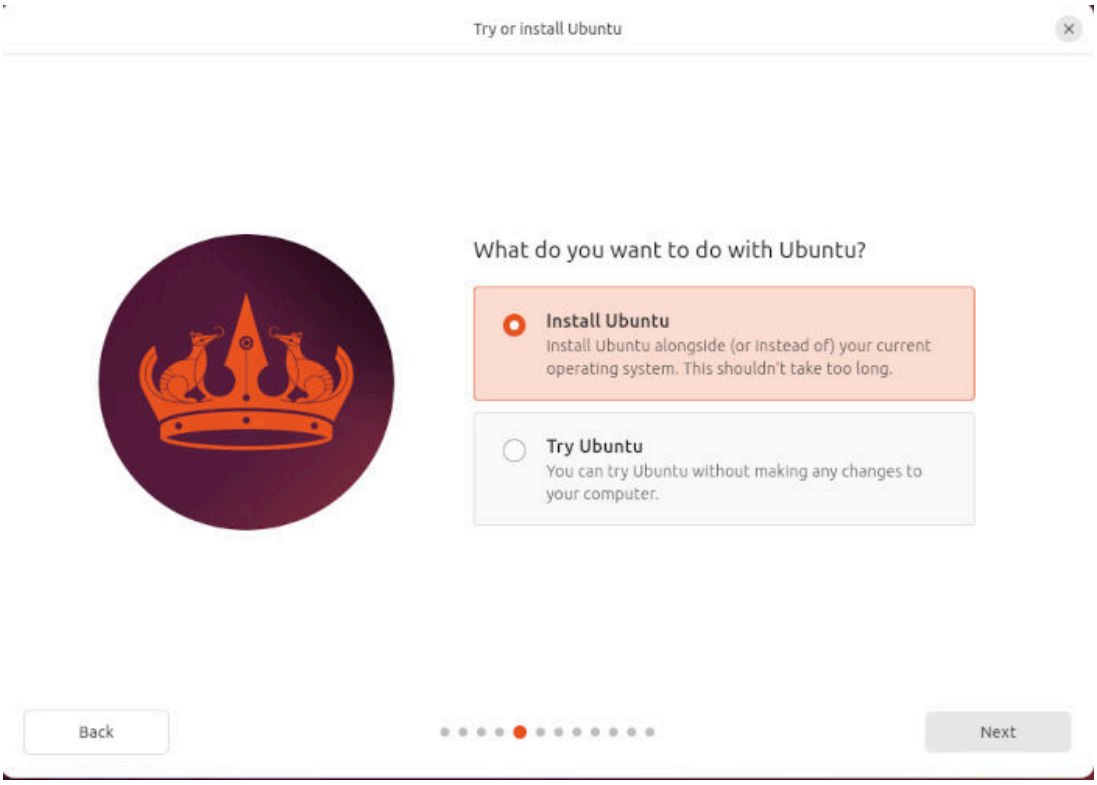
4.Updates available

Choose whether to install updates during installation to ensure the system is up to date with the latest security patches, bug fixes, and feature improvements. Alternatively, select Skip to update after the installation is complete.



5.Installation type

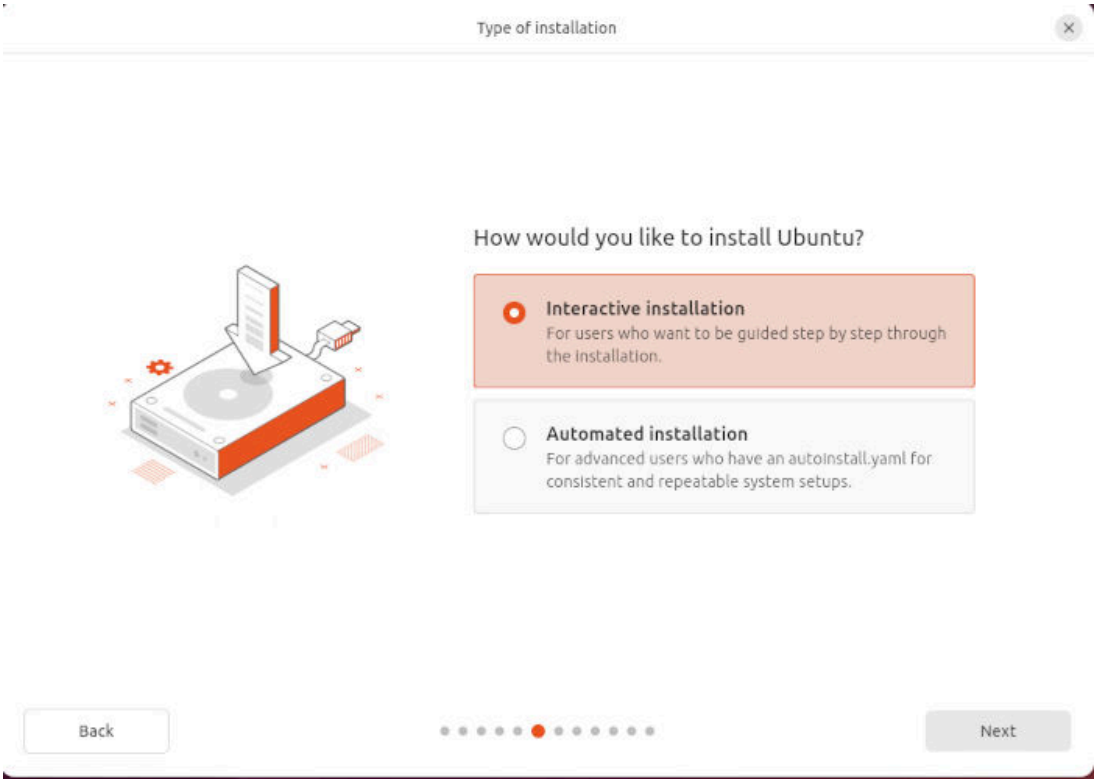
Install Ubuntu alongside the current operating system allows Ubuntu to coexist with an existing OS, preserving its files and settings.



6.Ubuntu Installation Method

Select the installation approach:

- Interactive Installation - Guides the user step by step through configuration options including partitions, user accounts, and software selection.
- Automated Installation - Uses predefined settings to install Ubuntu with minimal user input.

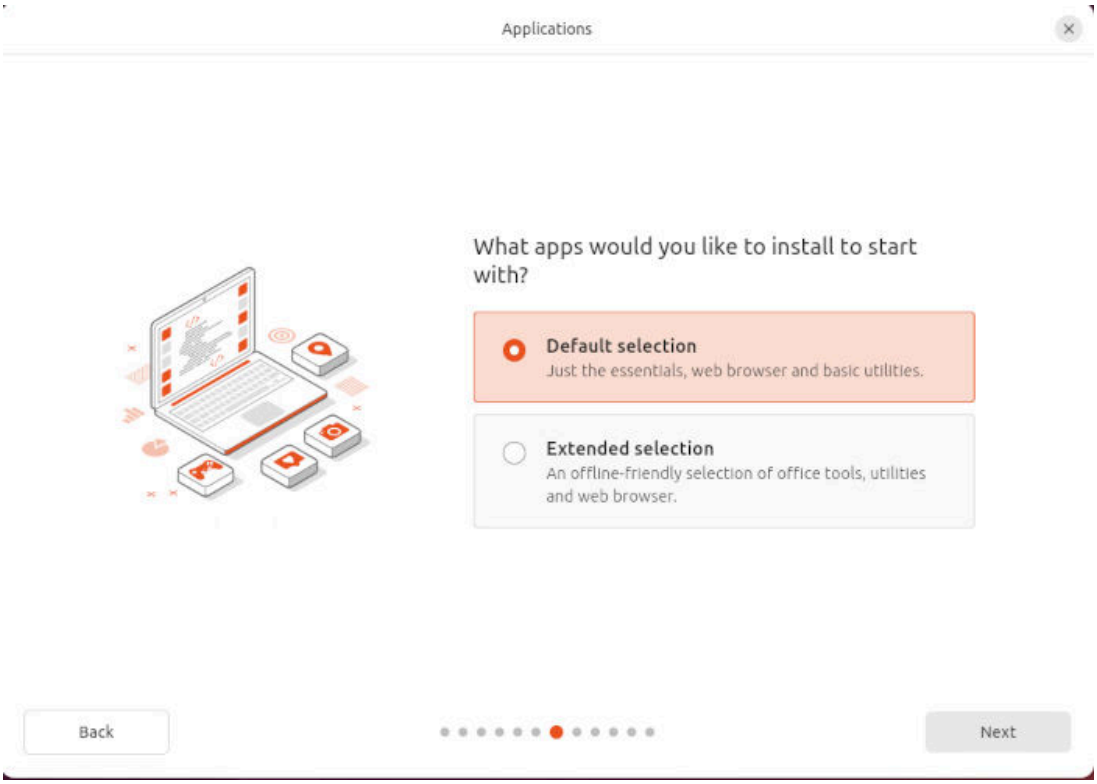


7.Application Selection

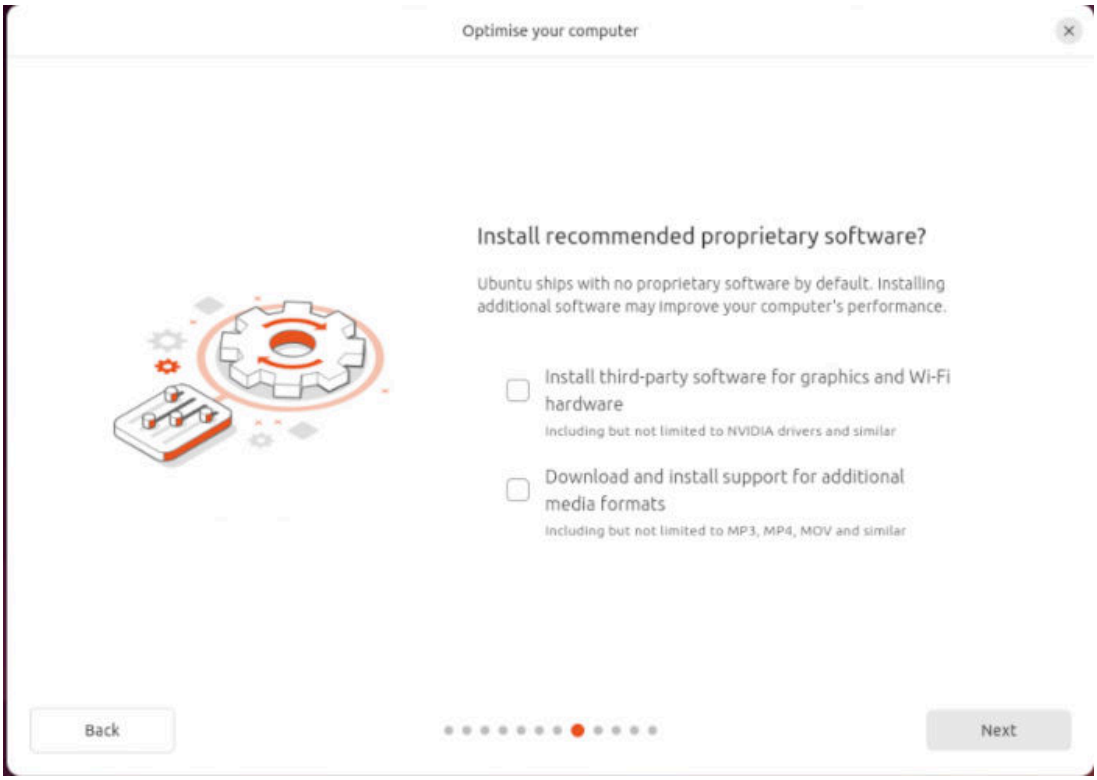
Choose between Default Selection or Extended Selection for pre-installed applications:

- Default Selection - Installs only essential applications for a basic Ubuntu environment.

- Extended Selection - Installs additional software, including office suites, media players, and other utilities.



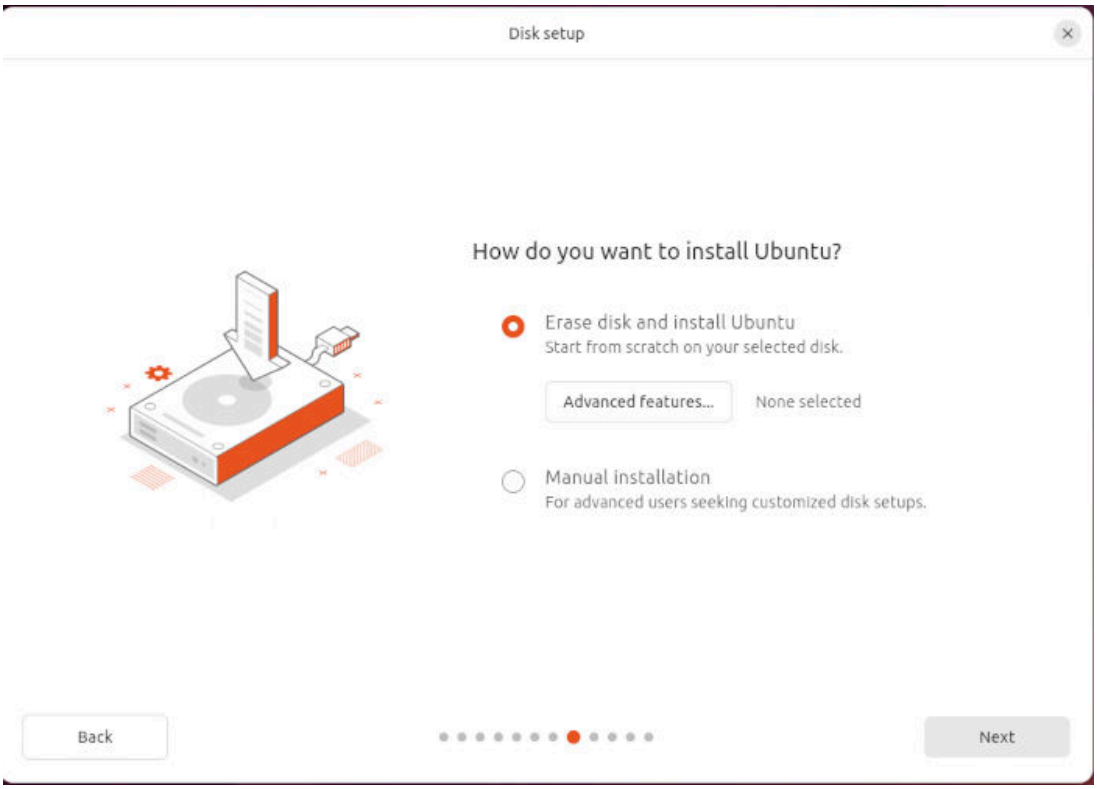
8.Install Recommended Proprietary Software



9.Installation Method

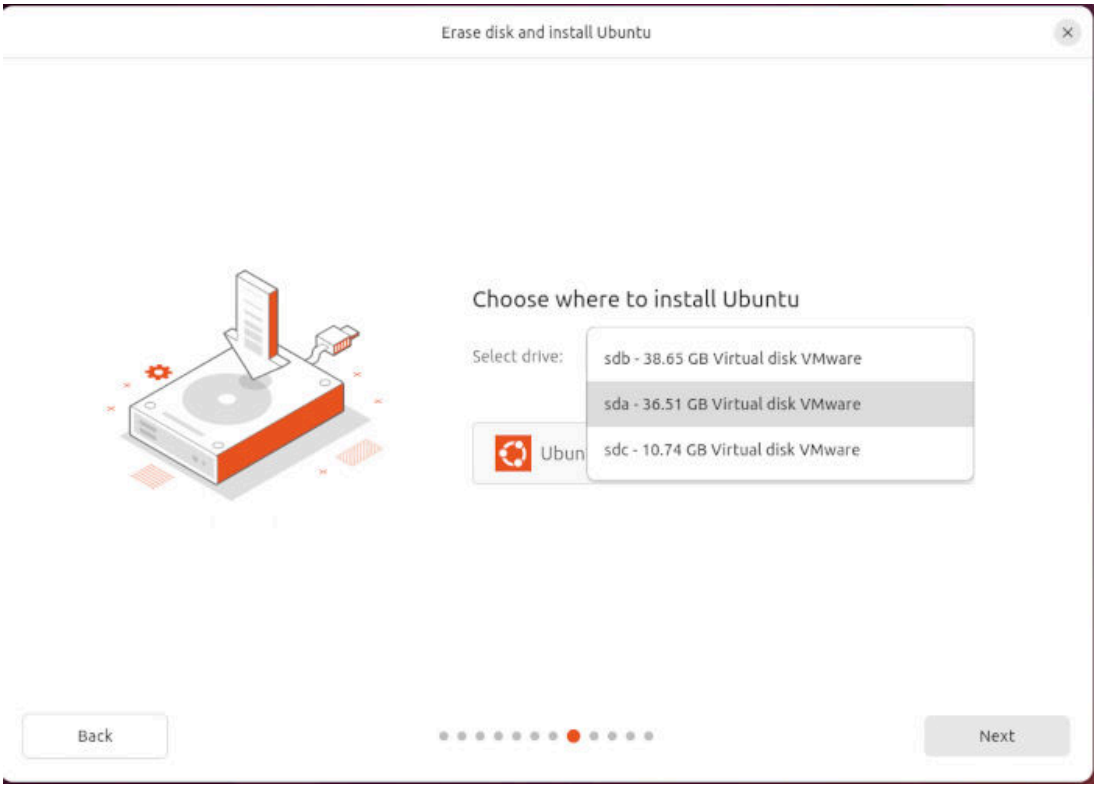
Choose how Ubuntu will be installed:

- Erase disk and install Ubuntu – Installs a fresh system by formatting the selected disk.
- Manual Installation ("Something else") – Allows custom partitioning, mount points, and disk selection.



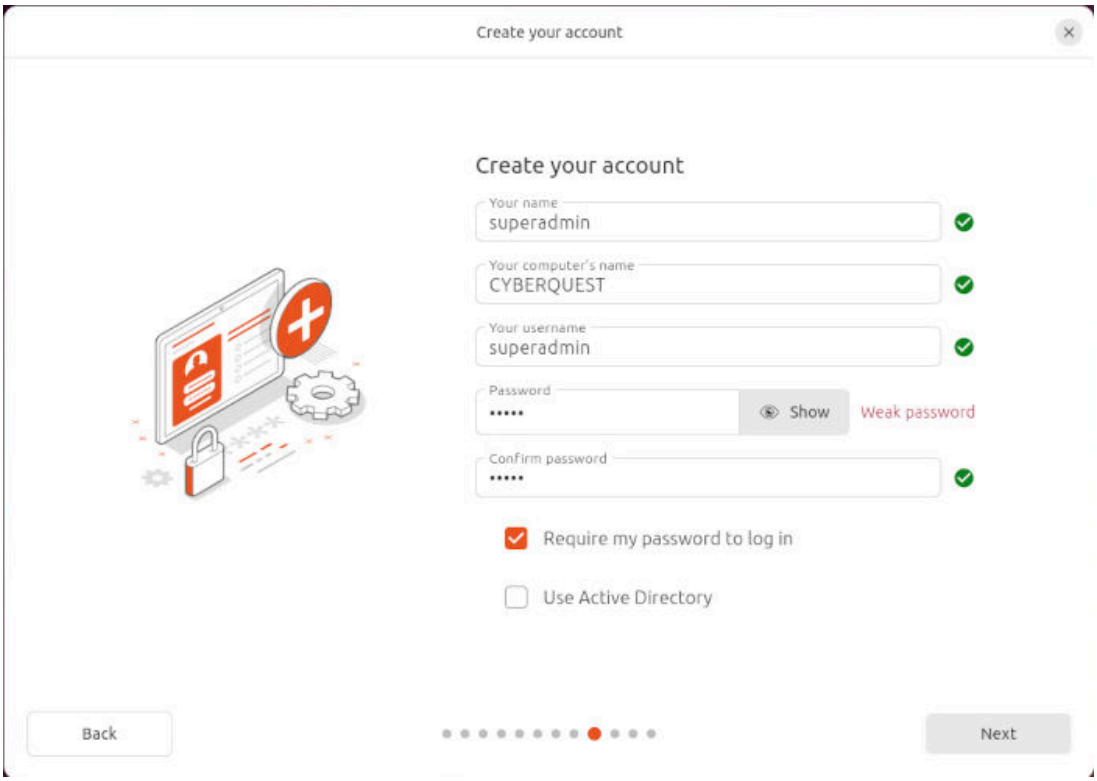
10.Select Installation Location

Specify the disk or partition where Ubuntu will be installed, ensuring the system is placed on the desired storage device.



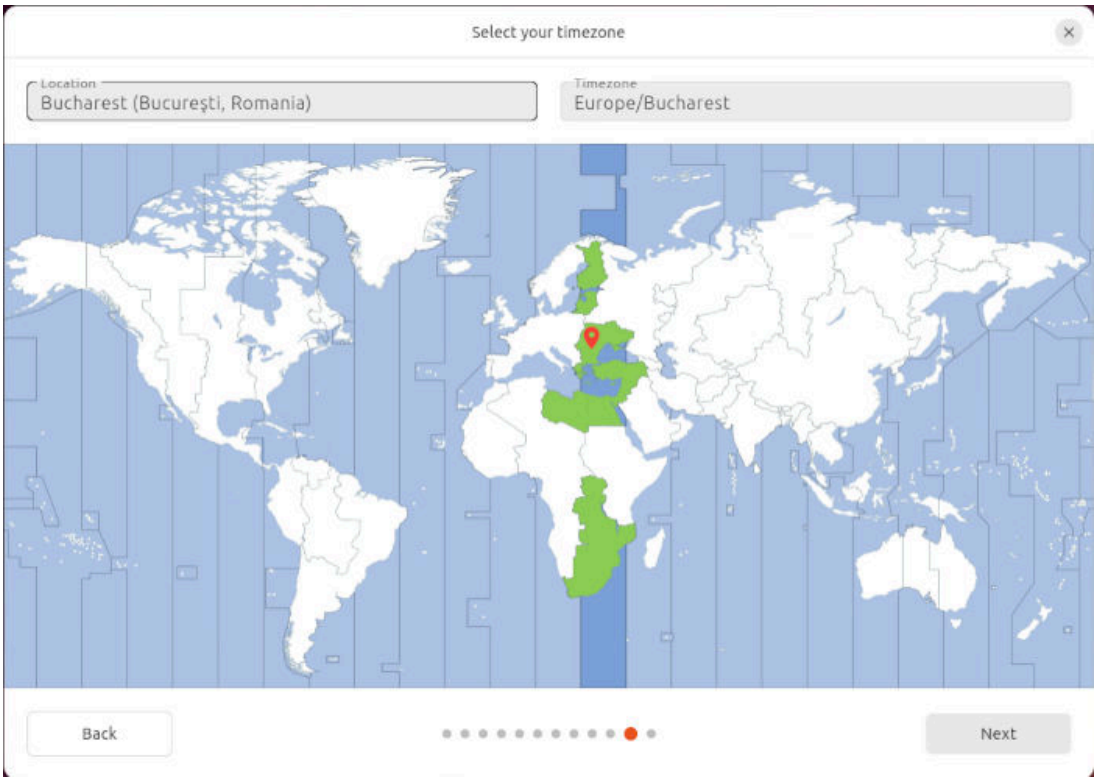
11.Create a User Account

Set up a user account by providing a full name, username, and password.



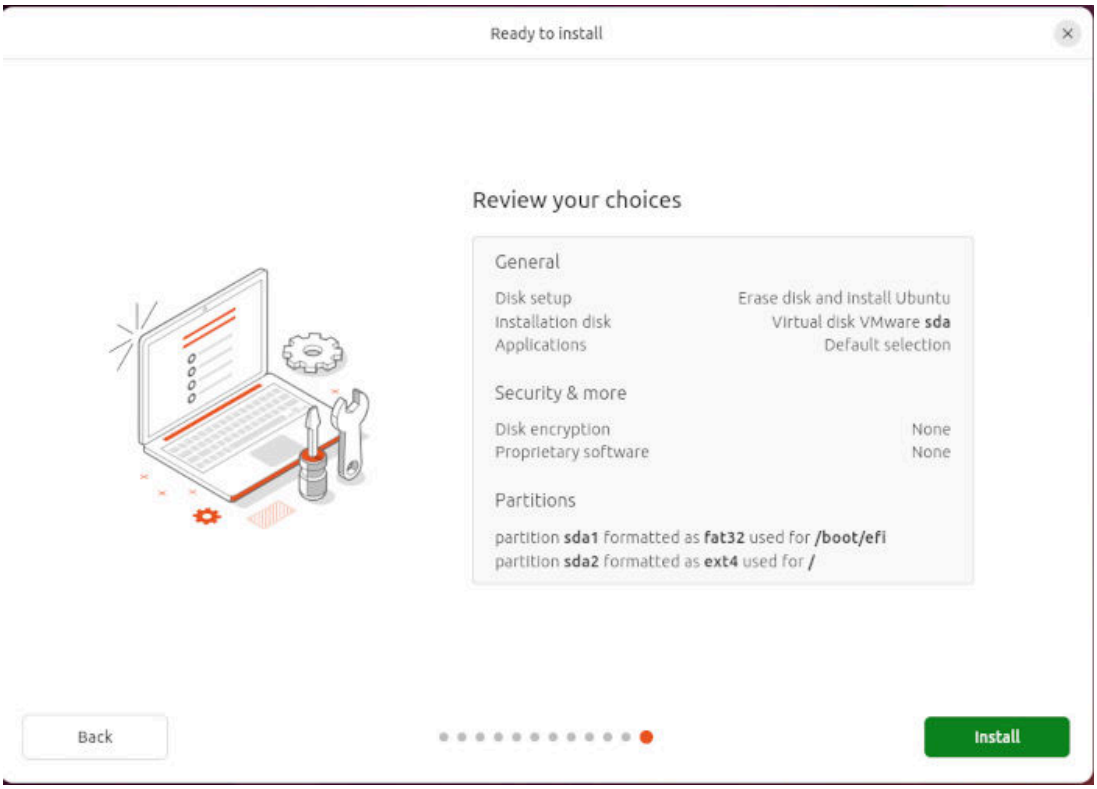
12.Select timezone

Choose the appropriate timezone for the system to ensure correct time and date settings.



13.Ready to Install - Review and Confirm

Review all installation settings, including disk partitions, user account, timezone, and software selections. Once confirmed, proceed to install Ubuntu on the system.



Once the installation is complete, a confirmation message is displayed. The system can now be restarted or testing can continue immediately, depending on the chosen action.

Distributed Architecture

Horizontal scaling through NoSQL service

Horizontal scaling is a strategy that CYBERQUEST users can use to enhance the performance of the server node by adding more instances of the server to your existing pool of servers so the load can be equally distributed. In horizontal scaling, the capacity of the individual server is not changed, but the load on the server is decreased. Horizontal scalability is achieved with the help of a distributed file system, clustering, and load balancing. Some of the reasons why businesses choose to scale horizontally include an increase in their I/O concurrency, need to reduce the load on existing nodes and to expand disk capacity. Horizontal-scaling is considerably easy as you can add more machines to the existing pool. It follows the partitioning of the data in which each node contains only one part of the data. For the NoSQL sevice that ensures horizontal scaling, CYBERQUEST uses Online DataStorage.

Introduction to Online DataStorage Clustering

Online DataStorage is built to be always available, and to scale with your needs. Scaling can come from deploying more performant servers, especially on CPU and memory considerations (vertical scale, or scaling up) or from deploying more servers (horizontal scale, or scaling out). While Online DataStorage can benefit from more powerful hardware, vertical scale has its limits. Real scalability comes from horizontal scale, the ability to add more nodes to the cluster and to spread load and reliability between them. With most databases, scaling horizontally usually requires a major overhaul of your application to take advantage of these extra boxes. By contrast, Online DataStorage is distributed by nature: it knows how to manage multiple nodes to provide scale and high availability. This also means that your application doesn't need to care about it. A **node** is a running instance of Online DataStorage, while a **cluster** consists of one or more nodes in the same **cluster.name**, that are working together to share their data and workload. As nodes are added to or removed from cluster, the cluster reorganizes itself to spread the data evenly.

Advantages of Online DataStorage clusters are:

1. Distributed data: In cluster data is distributed, replicated to another server. So, in case of failure of one node, data can be restored from replica node. It avoids single point of failure.

2. Dedicated node roles: Every node has dedicated role assigned to it, that ensures specific role and role-based load distribution hence increasing performance. Here are two important node roles
    - Data node: These nodes only store data and do data related operations, search and data manipulation.
    - Master node: Master of all nodes, it holds responsibility of overall cluster, addition and removal of nodes from cluster, keeping track of alive nodes, master reselection in appropriate cases.
3. Scalability: Cluster model is easily scalable to multiple no of nodes, thus increasing performance and reliability of Online DataStorage.

One node in cluster is elected to be the master node, being in charge of managing cluster-wide changes like creating/deleting an index or adding/removing a node from the cluster. The master node does not need to be involved in document-level changes or searches, which means that having just one master node will not become a bottleneck as traffic grows. Any node can become the master.

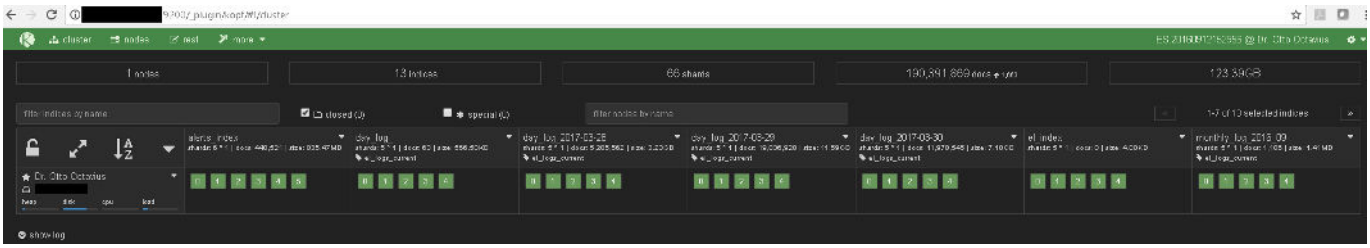
Every node knows where each document lives and can forward our request directly to nodes that hold the data we are interested in. Whichever node we talk to manages the process of gathering a response from the node or nodes holding data and returning the final response to client. All this is managed transparently by Online DataStorage.

CYBERQUEST takes advantage of this technology so whether the underlying database is clustered or single node deployment, **no additional configuration of CYBERQUEST is required.**

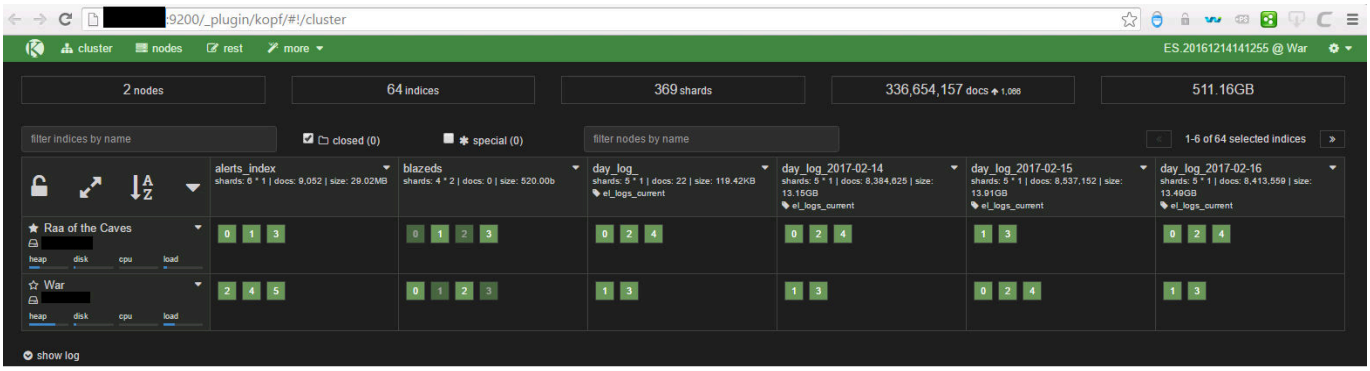
Checking cluster health

CYBERQUEST comes installed with the Online DataStorage. Cerebro service for a visual representation of the database, by accessing the CYBERQUEST IP address on port **9000** via a web browser.

The results are:



for a single node installation, or:



for two or more clustered nodes.

Adding cluster nodes

Out-of-the-box, Online DataStorage is configured to use unicast discovery to prevent nodes from accidentally joining a cluster. Only nodes running on the same machine will automatically form a cluster. To use unicast, you provide Online DataStorage with a list of nodes that it should try to contact. When a node contacts a member of the unicast list, it receives a full cluster state that lists all the nodes in cluster. It then contacts the master and joins the cluster.

This means your unicast list does not need to include all the nodes in your cluster. It just needs enough nodes that a new node can find someone to talk to. If you use dedicated masters, just list your three dedicated masters and call it a day. This setting is defined in **elasticsearch.yml** configuration file:

```
root@CyberQuest:~# nano /etc/elasticsearch//elasticsearch.yml
```

```
discovery.zen.ping.unicast.hosts:
["OtherEasticSearchHost1","OtherEasticSearchHost2"]
```

When finished, save and restart Online DataStorage service:

```
systemctl restart opensearch.service
```

Additional Online DataStorage documentation

Additional database documentation can be found here: **https://www.elastic.co/guide/en/elasticsearch/guide/master/index.html (https://www.elastic.co/guide/en/elasticsearch/guide/master/index.html)**

Horizontal scaling on MariaDB

Introduction

CYBERQUEST uses the MariaDB database for solution configuration data.

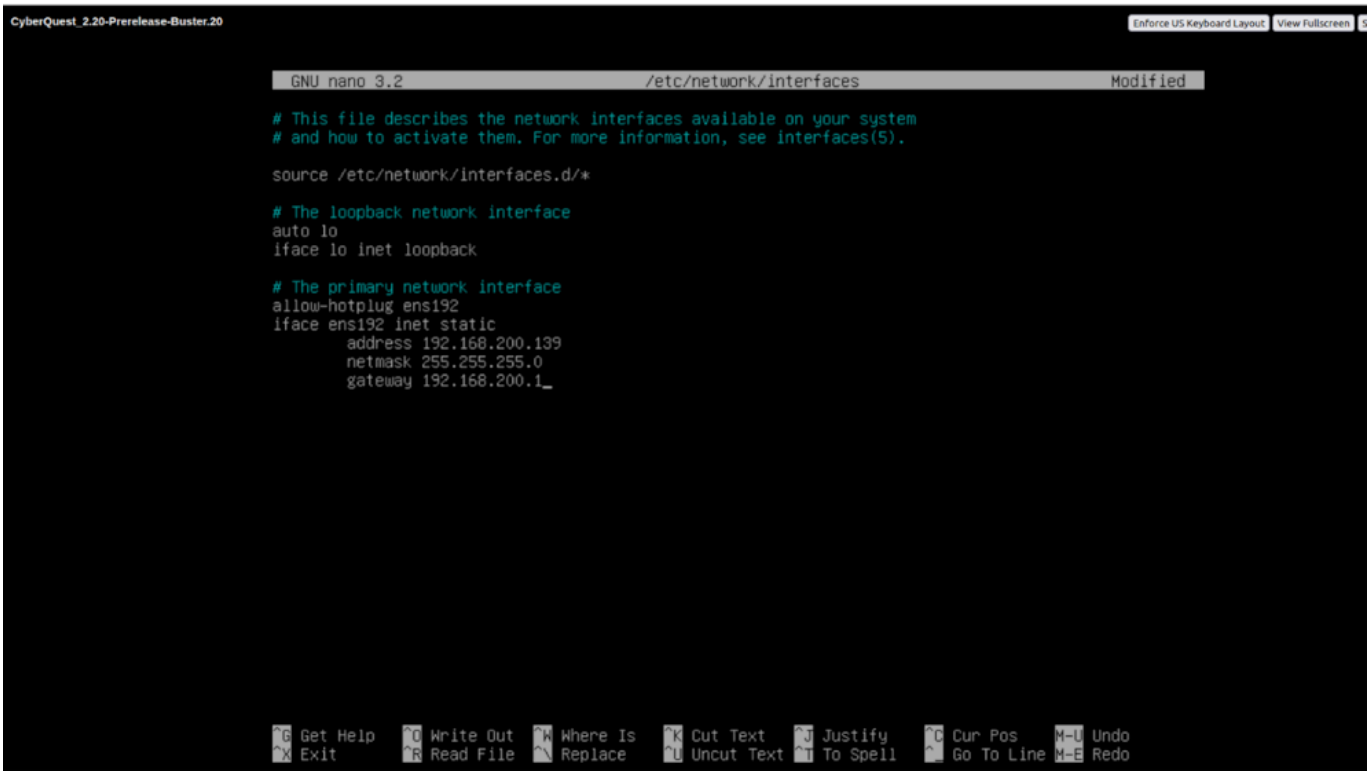
For High Availability architectures the MariaDB nodes are configured in a cluster.

The purpose of this document is to technically describe the MariaDB cluster configuration process. For the clustering we use MariaDB Galera Cluster (https://mariadb.com/kb/en/what-is-mariadb-galera-cluster/).

MariaDB cluster configuration

1. **Network interface configuration**

Make sure there are fixed ip's on all nodes

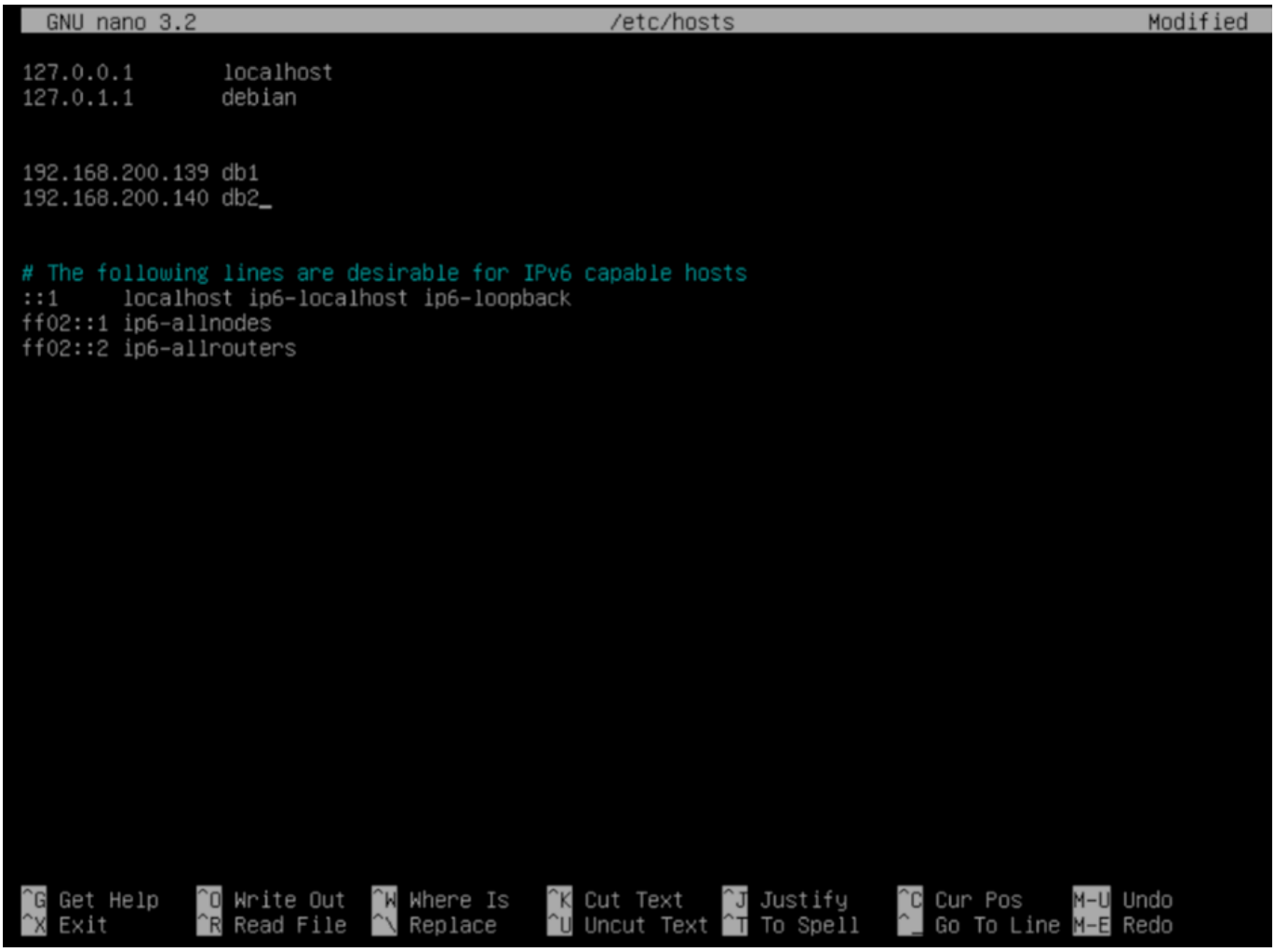


```
Ifdown ens192

Ifup ens192
```

Add in */etc/hosts* node records (on all nodes, in this case db1 and db2) *nano /etc/hosts*

```
nano /etc/hosts
```



2. **Configuring the *60-galera.conf file***

The clustering configuration file *60-galera.cnf* is node specific and is created manually - if it is not in */etc/mysql/mariadb.conf.d/*

- **Configuration file for machine 192.168.200.139 (db1)**

```
# * Galera-related settings
#
# See the examples of server wsrep.cnf files in /usr/share/mysql
# and read more at https://mariadb.com/kb/en/galera-cluster/

[galera]
# Mandatory settings
#wsrep_on = ON
#wsrep_provider =
#wsrep_cluster_address =
#binlog_format = row
#default_storage_engine = InnoDB
#innodb_autoinc_lock_mode = 2

# Allow server to accept connections on all interfaces.
#bind-address = 0.0.0.0

# Optional settings
#wsrep_slave_threads = 1
#innodb_flush_log_at_trx_commit = 0


[mysqld]
binlog_format=ROW
default-storage-engine=innodb
innodb_autoinc_lock_mode=2
bind-address=0.0.0.0

# Galera Provider Configuration
wsrep_on=ON
wsrep_provider=/usr/lib/galera/libgalera_smm.so

# Galera Cluster Configuration
wsrep_cluster_name="CQ_CLUSTER"
wsrep_cluster_address="gcomm://192.168.200.139,192.168.200.140"

# Galera Synchronization Configuration
wsrep_sst_method=rsync

# Galera Node Configuration
wsrep_node_address="192.168.200.139"
wsrep_node_name="db1"
```

- **Configuration file for machine 192.168.200.140 (db2)**

```
# * Galera-related settings
#
# See the examples of server wsrep.cnf files in /usr/share/mysql
# and read more at https://mariadb.com/kb/en/galera-cluster/

[galera]
# Mandatory settings
#wsrep_on = ON
#wsrep_provider =
#wsrep_cluster_address =
#binlog_format = row
#default_storage_engine = InnoDB
#innodb_autoinc_lock_mode = 2

# Allow server to accept connections on all interfaces.
#bind-address = 0.0.0.0

# Optional settings
#wsrep_slave_threads = 1
#innodb_flush_log_at_trx_commit = 0


[mysqld]
binlog_format=ROW
default-storage-engine=innodb
innodb_autoinc_lock_mode=2
bind-address=0.0.0.0

# Galera Provider Configuration
wsrep_on=ON
wsrep_provider=/usr/lib/galera/libgalera_smm.so

# Galera Cluster Configuration
wsrep_cluster_name="CQ_CLUSTER"
wsrep_cluster_address="gcomm://192.168.200.139,192.168.200.140"

# Galera Synchronization Configuration
wsrep_sst_method=rsync

# Galera Node Configuration
wsrep_node_address="192.168.200.140"
wsrep_node_name="db2"
```

3. **Final configuration**

- Copy the configuration file to */home/superadmin* on both nodes



- Mariadb services stop on both nodes



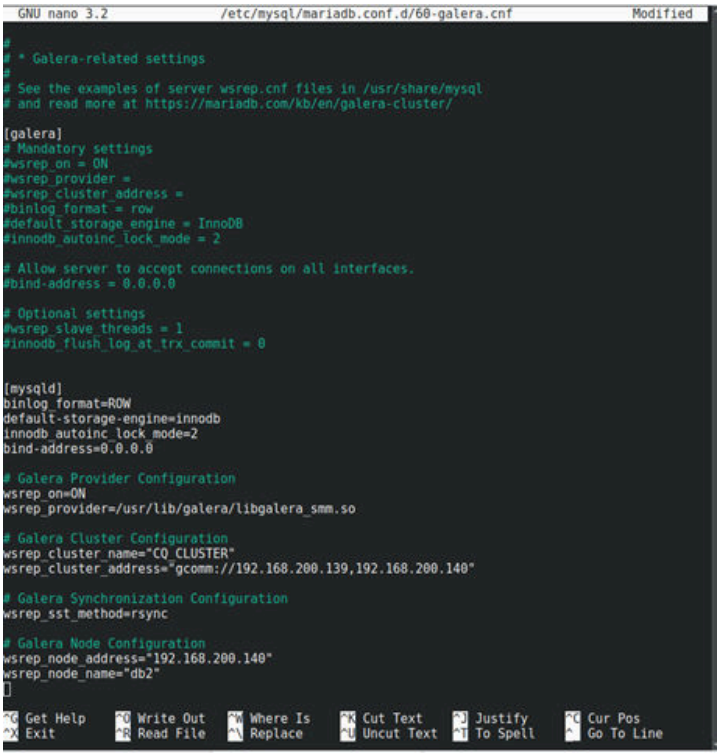
- Copy the configuration file to each node

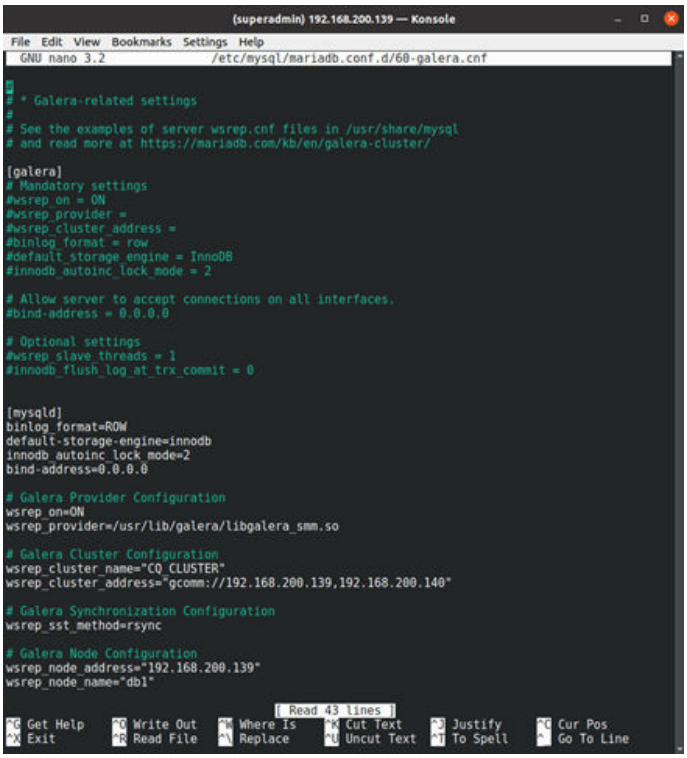
```
sudo cp /home/superadmin/60-galera.cnf /etc/mysql/mariadb.conf.d/
```

Checking the cluster

1. **Checking configurations**

Check the configuration in the file (on each node)





Bootstrap new cluster (on db1)

```
sudo galera_new_cluster
```

```
superadmin@debian:~$ sudo galera_new_cluster
superadmin@debian:~$ systemctl status ma
machine.slice    man-db.service   man-db.timer     mariadb.service
superadmin@debian:~$ systemctl status mariadb.service
● mariadb.service - MariaDB 10.3.27 database server
   Loaded: loaded (/lib/systemd/system/mariadb.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2021-06-18 12:53:22 EEST; 25s ago
     Docs: man:mysqld(8)
           https://mariadb.com/kb/en/library/systemd/
  Process: 25531 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d /var/run/mysqld (cod
  Process: 25532 ExecStartPre=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (co
  Process: 25534 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ] && VAR= ||   VAR=`c
  Process: 25691 ExecStartPost=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (c
  Process: 25693 ExecStartPost=/etc/mysql/debian-start (code=exited, status=0/SUCCESS)
 Main PID: 25655 (mysqld)
   Status: "Taking your SQL requests now..."
    Tasks: 42 (limit: 4700)
   Memory: 117.0M
   CGroup: /system.slice/mariadb.service
           └─25655 /usr/sbin/mysqld --wsrep-new-cluster --wsrep_start_position=00000000-0000-0
lines 1-16/16 (END)
```

Start the service on db2 (which is already configured):

```
sudo systemctl start mariadb.service
```

Check that the database statement has been received

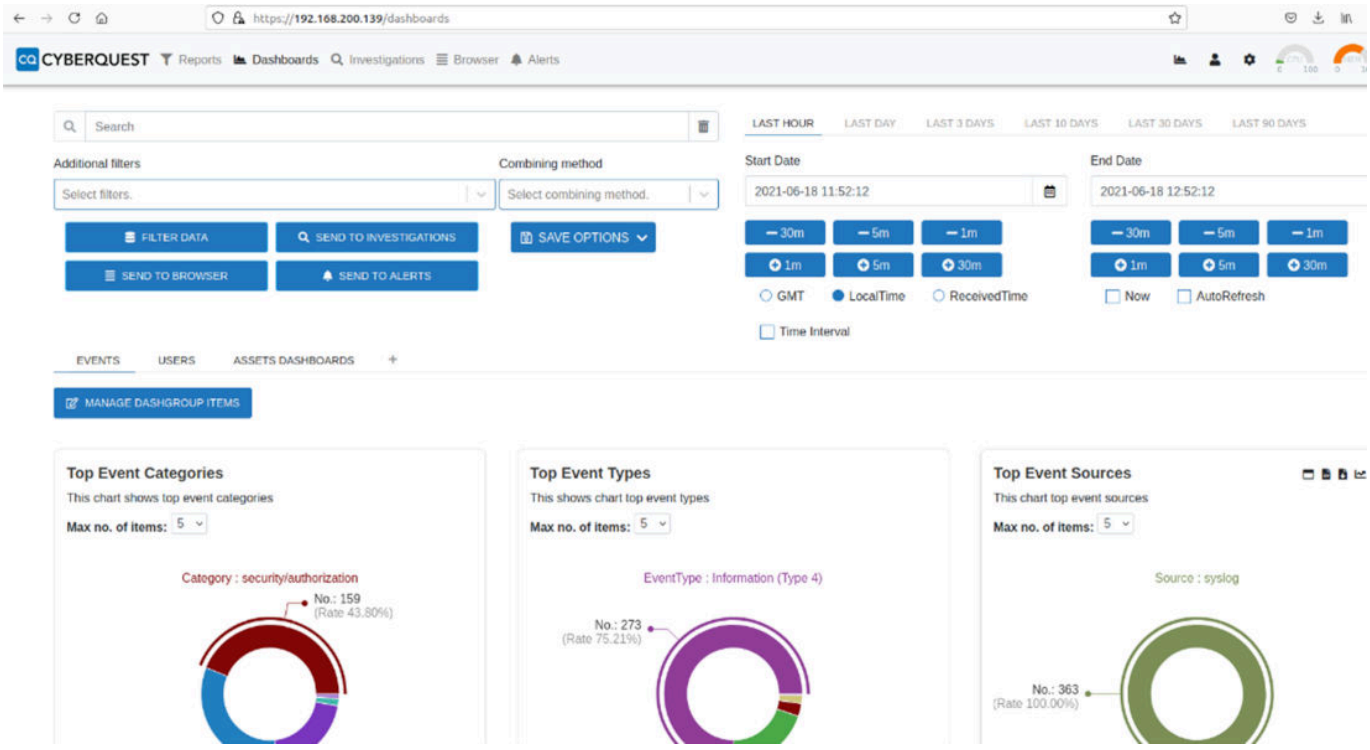
```
superadmin@debian:~$ sudo systemctl status mariadb.service
[sudo] password for superadmin:
● mariadb.service - MariaDB 10.3.27 database server
   Loaded: loaded (/lib/systemd/system/mariadb.service; enabled; vendor preset: enabled)
   Active: inactive (dead) since Fri 2021-06-18 12:34:08 EEST; 21min ago
     Docs: man:mysqld(8)
           https://mariadb.com/kb/en/library/systemd/
  Process: 630 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d /var/run/mysqld (code=
  Process: 663 ExecStartPre=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code
● mariadb.service - MariaDB 10.3.27 database server
   Loaded: loaded (/lib/systemd/system/mariadb.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2021-06-18 12:56:11 EEST; 7s ago
     Docs: man:mysqld(8)
           https://mariadb.com/kb/en/library/systemd/
  Process: 4289 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d /var/run/mysqld (code=exited, status=0/SU
  Process: 4290 ExecStartPre=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=exited, status=0/S
  Process: 4292 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ] && VAR= ||   VAR=`cd /usr/bin/..; /usr/b
  Process: 4565 ExecStartPost=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=exited, status=0/
  Process: 4567 ExecStartPost=/etc/mysql/debian-start (code=exited, status=0/SUCCESS)
 Main PID: 4413 (mysqld)
   Status: "Taking your SQL requests now..."
    Tasks: 42 (limit: 4700)
   Memory: 291.4M
   CGroup: /system.slice/mariadb.service
           └─4413 /usr/sbin/mysqld --wsrep_start_position=00000000-0000-0000-0000-000000000000:-1

jun 18 12:56:09 debian rsyncd[4507]: sent 1739 bytes  received 1225280 bytes  total size 1218647
jun 18 12:56:09 debian rsyncd[4504]: sent 2708 bytes  received 7942426 bytes  total size 7930277
jun 18 12:56:09 debian rsyncd[4516]: connect from db1 (192.168.200.139)
jun 18 12:56:09 debian rsyncd[4516]: rsync to rsync_sst/ from db1 (192.168.200.139)
jun 18 12:56:09 debian rsyncd[4516]: receiving file list
jun 18 12:56:09 debian rsyncd[4516]: sent 48 bytes  received 185 bytes  total size 41
jun 18 12:56:10 debian rsyncd[4470]: sent 0 bytes  received 0 bytes  total size 0
jun 18 12:56:11 debian systemd[1]: Started MariaDB 10.3.27 database server.
jun 18 12:56:11 debian /etc/mysql/debian-start[4569]: Upgrading MySQL tables if necessary.
jun 18 12:56:11 debian /etc/mysql/debian-start[4583]: Checking for insecure root accounts.
```

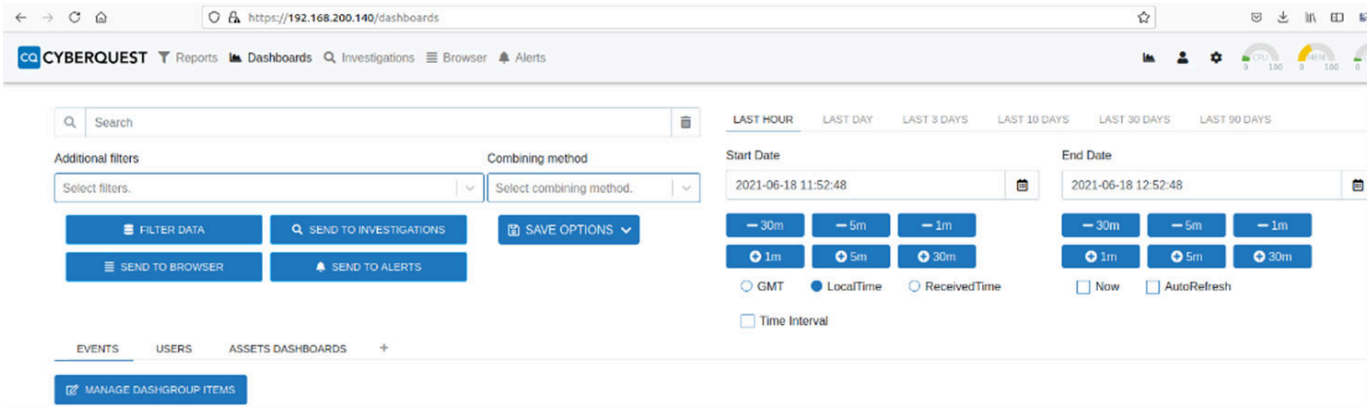
2. **GUI checking**

Check replication: when accessing the web interface, the configurations must be identical for the two CYBERQUEST machines.

db1:



db2:



You can see the identical configuration of dashgroups: *Events*, *Users*, *Asset Dashboards*.

This setup can also be used for failover purposes. When one database server is unavailable, the other has identical configuration.

HAProxy failover configuration

CyberQuest comes with HAProxy preinstalled. In order to accomodate High-Availability, Geo-Redundancies scenarios, Fail-Over configuraitons, additional settings need to be performed

Failover / Load Balancer scenario:

1. Edit /etc/haproxy/haproxy.cfg file to include Failover / Load Balancer configuration (on two nodes) to set it up

```
global
  log 127.0.0.1 local0 notice
  maxconn 10000
  user haproxy
  group haproxy
defaults
  timeout connect 5s
  timeout client 100s
  timeout server 100s
listen rabbitmq
  bind :5673
  mode tcp
  balance roundrobin
  server rabbitmq-01 <node1>:5672 check inter 5s rise 2 fall 3
  server rabbitmq-02 <node2>:5672 check inter 5s rise 2 fall 3
# optional, for proxying management site
frontend front_rabbitmq_management
  bind :15672
  default_backend back_rabbitmq_management
backend back_rabbitmq_management
  balance source
  server rabbitmq-mgmt-01 10.25.1.101:15673 check
  server rabbitmq-mgmt-02 10.25.1.102:15673 check
# optional, for monitoring
# listen stats :9000
#  mode http
#  stats enable
#  stats hide-version
# stats realm Haproxy\ Statistics
#  stats uri /
#  stats auth haproxy:haproxy
```

Configure CQ Services to use the Fail-Overed endpoint (see each service's configuration parameters).

Upgrades

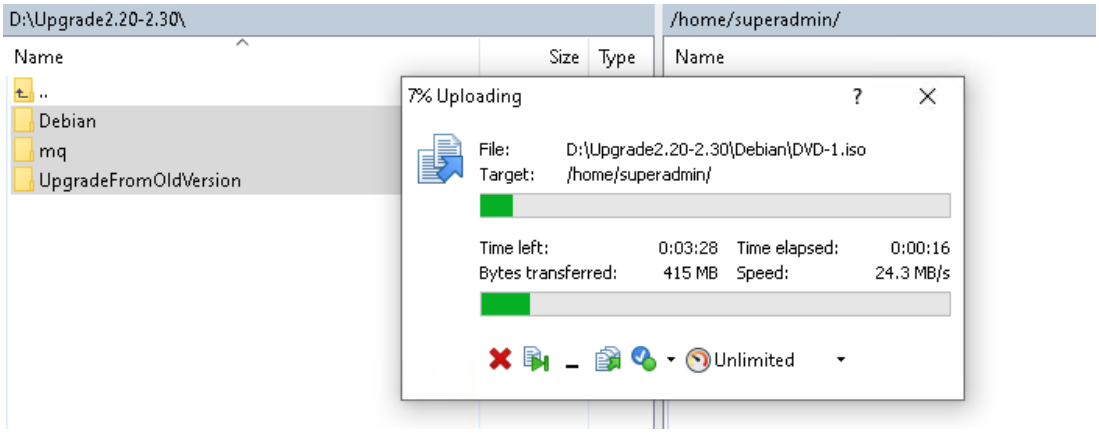
Upgrade CQ from V2.20 to V2.30

Prerequisites

- A CYBERQUEST 2.20 instance must be installed
- Back-up by creating a snapshot of the CYBERQUEST VM is recommended in this stage
- CYBERQUEST upgrade packets (https://download.cyberquestsolutions.ro/Upgrade2.20-2.30/Upgrade2.20-2.30.7z) must be downloaded prior to the beginning of the upgrade process

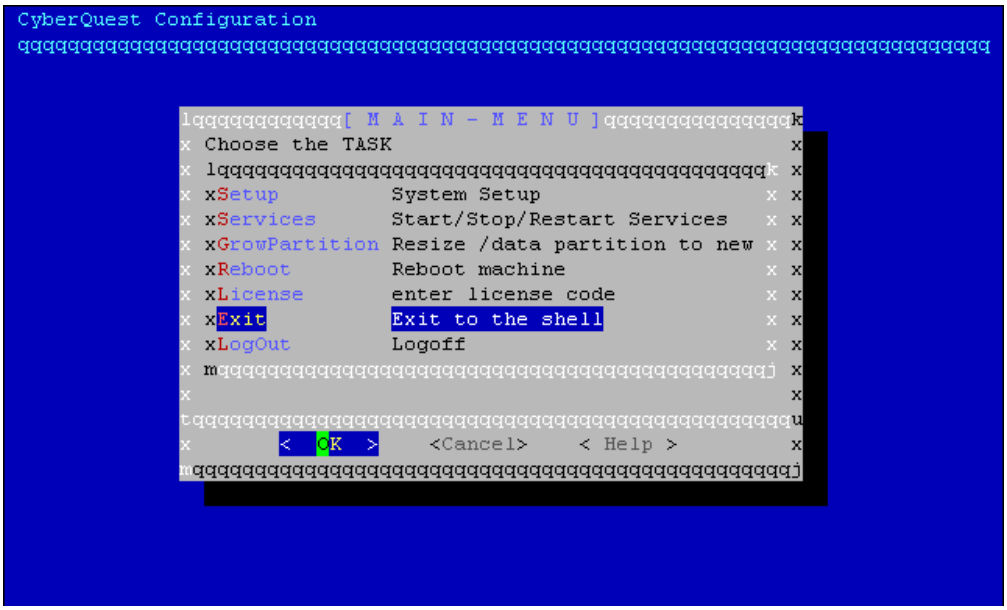
Technical operations

Using WinSCP, copy from **Upgrade2.20-2.30.7z** file the following folders: **Debian**, **mq** and **UpgradeFomOldVersion** to the CYBERQUEST server in the following path: **/home/superadmin/**



Access your CYBERQUEST instance via ssh and follow the steps bellow:

1.Login as **root** with password **toor1** and select **Exit** option



The result should look like this:



2.Create a new directory using th following command:

```
mkdir -p /media/iso1/
```

3.Edit the file **fstab**

A.Open the file **fstab** using the following command:

```
nano /etc/fstab
```

B.Add the following line of code at the end of the file:

```
/home/superadmin/Debian/DVD-1.iso /media/iso1/ udf,iso9660 loop 0 0
```

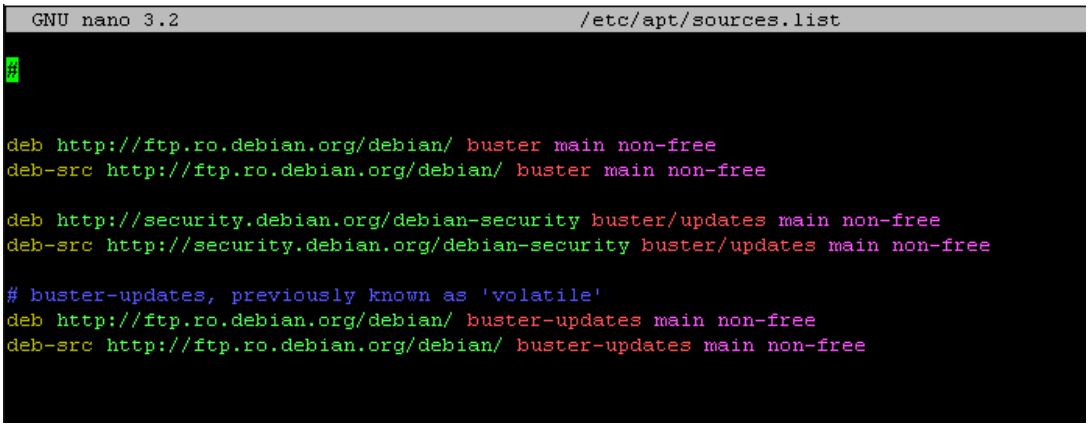
C.Save the file and exit.

4.Edit the file **sources.list**

A.Open the file **sources.list** using the following command:

```
nano /etc/apt/sources.list
```

B.Comment all lines in the file:



C.Add the following line of code at the end of the file:

```
deb [trusted=yes] file:/media/iso1/ bullseye main contrib
```

D.Save the file and exit.

5.Edit the file **php.list**

A.Open the file **php.list** using the following command:

```
nano /etc/apt/sources.list.d/php.list
```

B.Comment out the line in the file:

```
 GNU nano 3.2                                  /etc/apt/sources.list.d/php.list

deb https://packages.sury.org/php/ buster main
```

6.Edit the file **opendistroforelasticsearch.list**

A.Open the file **opendistroforelasticsearch.list** using the following command:

```
nano /etc/apt/sources.list.d/opendistroforelasticsearch.list
```

B.Comment out the line in the file:

```
 GNU nano 3.2                    /etc/apt/sources.list.d/opendistroforelasticsearch.list

deb https://d3g5vo6xdbdb9a.cloudfront.net/apt stable main
```

7.Mount ISO image using the following command:

```
mount -a
```

8.Update CYBERQUEST server using the following command:

```
apt-get update
```

9.Upgrade CYBERQUEST server to Debian 11

A.Upgrade CYBERQUEST server using the following command:

```
apt-get upgrade
```

B.Press **Y** on “Do you want to continue? [Y/n]” and Enter

```
  librest-0.7-0 libsasl2-2 libsasl2-modules libsasl2-modules-db libseccomp2 libselinux1 libsemanage-common
  libsemanage1 libsensors-config libsepol1 libsigsegv2 libsmartcols1 libsnappy1v5 libsnmp-base libss2
  libssh2-1 libssl-dev libssl1.1 libstemmer0d libswitch-perl libtext-wrapi18n-perl libthai-data libthai0
  libtimedate-perl libtinfo5 libtinfo6 libunistring2 liburi-perl libuuid1 libwayland-cursor0 libwayland-egl1
  libx11-6 libx11-data libx11-dev libx11-xcb1 libxau-dev libxau6 libxaw7 libxcb-dri2-0 libxcb-dri3-0
  libxcb-glx0 libxcb-present0 libxcb-render0 libxcb-shape0 libxcb-shm0 libxcb-sync1 libxcb1 libxcb1-dev
  libxcomposite1 libxcursor1 libxdamage1 libxext6 libxfixes3 libxi6 libxkbcommon0 libxmlsec1
  libxmlsec1-openssl libxt-dev libxt6 libyaml-0-2 libzip4 libzstd1 linux-libc-dev logrotate lsb-base
  lsb-release lsof make manpages manpages-dev mariadb-common mlocate mount mysql-common nano ncurses-base
  ncurses-bin ncurses-term net-tools netbase netcat-traditional ntp openssl os-prober patch pinentry-curses
  powermgmt-base psmisc python-apt-common python-pip-whl python3-asn1crypto python3-certifi python3-chardet
  python3-cryptography python3-debconf python3-debian python3-debianbts python3-distro-info python3-httplib2
  python3-idna python3-pip python3-pkg-resources python3-pysimplesoap python3-reportbug python3-requests
  python3-setuptools python3-software-properties python3-urllib3 python3-wheel python3-xdg readline-common
  reportbug sensible-utils shared-mime-info socat software-properties-common ssl-cert sudo systemd-sysv
  sysvinit-utils tar task-english task-ssh-server tasksel tasksel-data tcpdump telnet traceroute tzdata ucf
  unzip vim-common vim-tiny wamerican whiptail x11-common x11proto-core-dev x11proto-dev x11proto-input-dev
  xauth xkb-data xorg-sgml-doctools xtrans-dev xxd xz-utils zlib1g zlib1g-dev
365 upgraded, 0 newly installed, 0 to remove and 233 not upgraded.
Need to get 0 B/109 MB of archives.
After this operation, 20.5 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

C.Press **q** button

```
apt-listchanges: News
---------------------

apt (2.1.16) unstable; urgency=medium

  Automatically remove unused kernels on apt (dist,full)-upgrade. To revert
  to previous behavior, set APT::Get::AutomaticRemove::Kernels to false or
  pass --no-auto-remove to the command. apt-get remains unchanged.

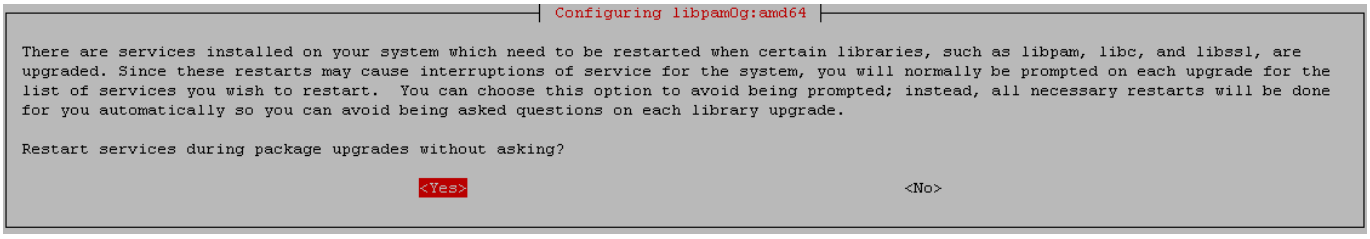
  Packages files can now set the Phased-Update-Percentage field to restrict
  update rollout to a specified percentage of machines. Previously, this has
  only been available to users of Ubuntu's update-manager tool. See
  apt_preferences(5) for details and how to configure multiple systems to get
  the same updates. Phased updates are disabled in chroots for now to not
  break buildd-style setups.

 -- Julian Andres Klode <jak@debian.org>  Fri, 08 Jan 2021 22:01:50 +0100

apt (1.9.11) experimental; urgency=medium

  apt(8) now waits for the lock indefinitely if connected to a tty, or
:
```

D.Select **Yes** on “Restart services during package upgrades without asking?” and Enter



10.Upgrade CYBERQUEST server

A.Upgrade CYBERQUEST server using the following command:

```
apt-get dist-upgrade
```

B.Press **Y** on “Do you want to continue? [Y/n]” and Enter

```
  libhttp-message-perl libidn2-0 libiptc0 libirs161 libisccc161 libisccfg163 libitm1 libjemalloc2 liblcms2-2
  libldap-2.4-2 liblocale-gettext-perl liblsan0 liblwres161 libnginx-mod-http-geoip
  libnginx-mod-http-image-filter libnginx-mod-http-xslt-filter libnginx-mod-mail libnginx-mod-stream
  libnspr4 libnss-systemd libp11-kit0 libpackagekit-glib2-18 libpam-modules libpam-modules-bin
  libpam-systemd libpango-1.0-0 libpangocairo-1.0-0 libpangoft2-1.0-0 libpci3 libpixman-1-0 libpng16-16
  libpolkit-agent-1-0 libpolkit-gobject-1-0 libproxy1v5 libpulse0 libpython2-stdlib libpython2.7-minimal
  libpython2.7-stdlib libpython3-dev libpython3-stdlib libquadmath0 librabbitmq4 librsvg2-2 librsvg2-common
  librtmp1 libsensors5 libslang2 libsndfile1 libsoup-gnome2.4-1 libsoup2.4-1 libsqlite3-0 libstdc++6
  libsystemd0 libtasn1-6 libterm-readkey-perl libtext-charwidth-perl libtext-iconv-perl libtiff5 libtsan0
  libubsan1 libuchardet0 libudev1 libunbound8 libvorbis0a libvorbisenc2 libwayland-client0 libwebp6 libwrap0
  libxapian30 libxml2 libxslt1.1 libxtables12 linux-image-amd64 locales login man-db mariadb-server mawk mc
  mc-data mime-support nftables nginx nginx-common open-vm-tools openssh-client openssh-server
  openssh-sftp-server packagekit packagekit-tools passwd pciutils perl perl-base php7.4-cli php7.4-common
  php7.4-curl php7.4-gd php7.4-json php7.4-mbstring php7.4-mysql php7.4-opcache php7.4-readline php7.4-xml
  pigz policykit-1 procps python2 python2-minimal python2.7 python2.7-minimal python3 python3-apt
  python3-cffi-backend python3-dbus python3-dev python3-distutils python3-gi python3-keyring python3-lib2to3
  python3-minimal python3-pycurl python3-secretstorage python3-six rsync rsyslog snmp snmpd sntp systemd
  udev unattended-upgrades util-linux util-linux-locales wget x11-utils
232 upgraded, 101 newly installed, 39 to remove and 0 not upgraded.
Need to get 0 B/291 MB of archives.
After this operation, 533 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

C.Press **q** button

```
apt-listchanges: News
---------------------

bsdmainutils (12.1.1) unstable; urgency=medium

  The "calendar" program, formerly provided in this package, now appears in
  the separate package "calendar".

  The tools "col", "colrm", "column", "hexdump", and "ul" are now provided as
  "bsdextrautils" from the util-linux sources.

 -- Michael Meskes <meskes@debian.org>  Wed, 27 May 2020 17:05:02 +0200

bsdmainutils (12.1.3) unstable; urgency=medium

  The tools "look" and "write" are also now part of "bsdextrautils" from the
  util-linux sources.

  The "from", "printerbanner", and "lorder" programs are discontinued. The
  "mailutils" package contains an alternative implementation of "from".

:
```

D.Press **Enter** on "rsyslog.conf (Y/I/N/O/D/Z) [default=N] ?"

```
Setting up libglib2.0-0:amd64 (2.66.8-1) ...
Setting up libmaxminddb0:amd64 (1.5.2-1) ...
Setting up perl-modules-5.32 (5.32.1-4+deb11u2) ...
Setting up libbrotli1:amd64 (1.0.9-2+b2) ...
Setting up libsqlite3-0:amd64 (3.34.1-3) ...
Setting up libpango-1.0-0:amd64 (1.46.2-3) ...
Setting up libcbor0:amd64 (0.5.0+dfsg-2) ...
Setting up libgdk-pixbuf2.0-common (2.42.2+dfsg-1+deb11u1) ...
Setting up rsyslog (8.2102.0-2+deb11u1) ...
Installing new version of config file /etc/logcheck/ignore.d.server/rsyslog ...
Installing new version of config file /etc/logrotate.d/rsyslog ...

Configuration file '/etc/rsyslog.conf'
 ==> Modified (by you or by a script) since installation.
 ==> Package distributor has shipped an updated version.
   What would you like to do about it ?  Your options are:
    Y or I  : install the package maintainer's version
    N or O  : keep your currently-installed version
      D     : show the differences between the versions
      Z     : start a shell to examine the situation
 The default action is to keep your current version.
*** rsyslog.conf (Y/I/N/O/D/Z) [default=N] ?
```

E.Press **Enter** on "sysctl.conf (Y/I/N/O/D/Z) [default=N] ?"

```
Setting up libjs-sphinxdoc (3.4.3-2) ...
Setting up gpg-wks-server (2.2.27-2+deb11u2) ...
Setting up mariadb-client-10.5 (1:10.5.18-0+deb11u1) ...
Installing new version of config file /etc/mysql/mariadb.conf.d/50-client.cnf ...
Installing new version of config file /etc/mysql/mariadb.conf.d/50-mysql-clients.cnf ...
Setting up open-vm-tools (2:11.2.5-2+deb11u1) ...
Installing new version of config file /etc/vmware-tools/vgauth.conf ...
Setting up groff-base (1.22.4-6) ...
Setting up cpp (4:10.2.1-1) ...
Setting up libhtml-parser-perl (3.75-1+b1) ...
Setting up procps (2:3.3.17-5) ...

Configuration file '/etc/sysctl.conf'
 ==> Modified (by you or by a script) since installation.
 ==> Package distributor has shipped an updated version.
   What would you like to do about it ?  Your options are:
    Y or I  : install the package maintainer's version
    N or O  : keep your currently-installed version
      D     : show the differences between the versions
      Z     : start a shell to examine the situation
 The default action is to keep your current version.
*** sysctl.conf (Y/I/N/O/D/Z) [default=N] ?
```

11.Unmask the RabbitMQ and restart the service

A.Unmask the RabbitMQ service using the following command:

```
systemctl unmask rabbitmq-server.service
```

B.Restart RabbitMQ service

```
systemctl restart rabbitmq-server.service
```

12.Install RabbitMQ packets

A.Go to the path **/home/superadmin/mq/** using the following command:

```
cd /home/superadmin/mq
```

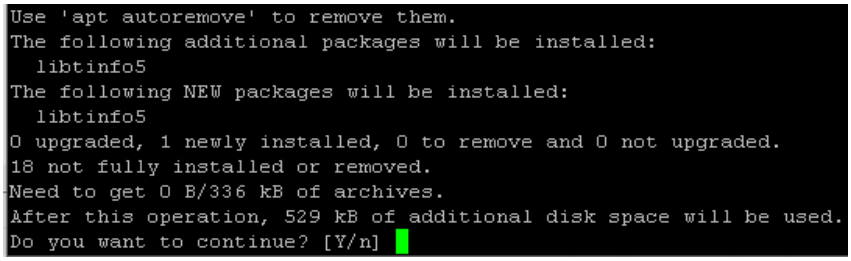
B.Install packages using the following command:

```
dpkg -i *
```

C.Automatically resolve installation issues using the following command:

```
apt-get -f install
```

D.Press **Y** on “Do you want to continue? [Y/n]” and Enter



E. Restart RabbitMQ service

```
systemctl restart rabbitmq-server.service
```

13.Update Web Application and services

A.Change the path to: **/home/superadmin/UpgradeFromOldVersion** using the following command:

```
cd /home/superadmin/UpgradeFromOldVersion
```

B.Run the script **Script.sh** using the following command:

```
bash Script.sh "mysql database password"
```

C.Press **Enter** on “lic (Y/I/N/O/D/Z) [default=N] ?”

```
  libssl-dev libtasn1-doc libunbound8 libwayland-cursor0 libwayland-egl1 libxkbcommon0
  linux-image-4.19.0-12-amd64 mariadb-server nettle-dev python2 python2-minimal python3-asn1crypto
  python3-entrypoints python3-jeepney python3-keyring python3-secretstorage python3-xdg python3.7-minimal
  snmp x11proto-input-dev x11proto-kb-dev
Use 'apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Unpackaging dataacquisition\n\n\n\n
(Reading database ... 90462 files and directories currently installed.)
Preparing to unpack data-acquisition-2.30.39-debian_buster.deb ...
Unpacking data-acquisition (2.30.39) over (2.20.285) ...
Setting up data-acquisition (2.30.39) ...

Configuration file '/var/opt/cyberquest/dataacquisition/conf/lic'
 ==> Modified (by you or by a script) since installation.
 ==> Package distributor has shipped an updated version.
   What would you like to do about it ?  Your options are:
    Y or I  : install the package maintainer's version
    N or O  : keep your currently-installed version
      D     : show the differences between the versions
      Z     : start a shell to examine the situation
 The default action is to keep your current version.
*** lic (Y/I/N/O/D/Z) [default=N] ?
```

12.Return to the default settings for data correlation and data storage services, then delete the assets table

A.Connect to the mysql database using the command below and enter the mysql database password

```
mysql -u root -p;
```

B.Return to default settings for Data Storage service

```
delete from config.settings where name like 'DataStorage%';
```

C.Return to default settings for Data Correlation service

```
delete from config.settings where name like 'DataCorrelation%';
```

D.Delete content from **assets** table

```
use reports;
```

```
truncate table assets;
```

E. Disconnect from the MySQL database using the **CTRL+D** keys.

F.Restart services

```
systemctl restart data-storage.service data-correlation.service data-acquisition.service
```

12.Logon to web interface and check the **About** page in **Settings**:

	Version	Build
WebApplication	2.30.71	2023-03-08 14:42:23
DataAcquisition	2.30.39.	2023-03-27 07:29:40
DataServer	2.30.6.	2023-01-25 14:03:56
DataStorage	2.30.17	2022-11-25 17:46:05
Administration	2.30.12	2022-11-21 17:33:33
DataCorrelation	2.30.33.	2023-03-27 10:52:53

Data Sources

Introduction

CYBERQUEST is a Data Security Analytics solution and is delivered as a physical or virtual appliance (integrated software solution - operating system package) on the Linux Debian platform.

Main features:

- It can collect audit events from any environment / any format: Syslog, Windows, from files (.csv, .txt, .log etc.), from database tables, metadata (NetFlow, sFlow) etc.
- Contains default built-in connectors for most common data sources (MS Windows and Unix-like operating systems, network equipment, databases, etc.).
- Allows the creation of dedicated connectors for specific data sources
- Inserts all data streams or only specific collected data streams into the correlation engine
- Allows the creation of dashboards and reports
- Logging into the application can be done using the Active Directory account and as an additional measure, 2FA authentication can be added
- Provides a proprietary DTS (Data Transformation Services) module through which it performs additional transformations on data extracted from collected events
- Allows the creation of real-time alerts and their customization according to the beneficiary's requirements

Tag based Parsing

Internal CQ DataFlow

Data is collected from various sources using CYBERQUEST's Collecting Agent (WMI, ODBC or file-level gathering etc.), or receiving data flows (syslog, NetFlow etc.). Data is organized in queues, sent to a Data Acquisition Service (DAS), which applies acquisition rules and then sends raw data to a Data Transformation Service (DTS). DTS is responsible for parsing data and generate real-time alerts.

Data Server - is responsible for receiving events and pre-processing them. After this process, the events are sent to the Data Acquisition service using the internal queue service (RabbitMQ).

Windows Agent - send events from Windows stations to the Data Acquisition service using the internal queuing service (RabbitMQ).

RabbitMQ - is responsible for the internal queue management of the application.

Data Acquisition - it processes events using API parsers. After the events have been processed, they are sent to: online database (Online DataStorage), Data Storage service and Data Correlation service.

Data Storage - this service encrypts and compresses events in the archive. The Data Storage service allows the CYBERQUEST application to maintain huge archive repositories. In projects where data needs to be kept for very long periods of time and with immediate access requirements.

Data Correlation - generate alerts based on **real time** and correlate events for alerting.

Elastisearch - is the online database.

Automatic parsing

Automatic parsing is performed by the Data Server service together with the Data Acquisition service.

The Data Server service receives events, pre-processes them and sends them to the Data Acquisition service for processing.

Events that have been pre-processed by the Data Server are given a tag and Data Acquisition processes them according to the tag given by the Data Server.

If the events have not been pre-processed by the Data Server, they will not be processed by the Data Acquisition service and the following must be added data source for that event type. Data sources can be added from the web application in the **Settings -> Management -> Data Source Manager** page.

Tag Alias

Tag alias is a function that allows parsing events using a parser other than the original one given by the data server.

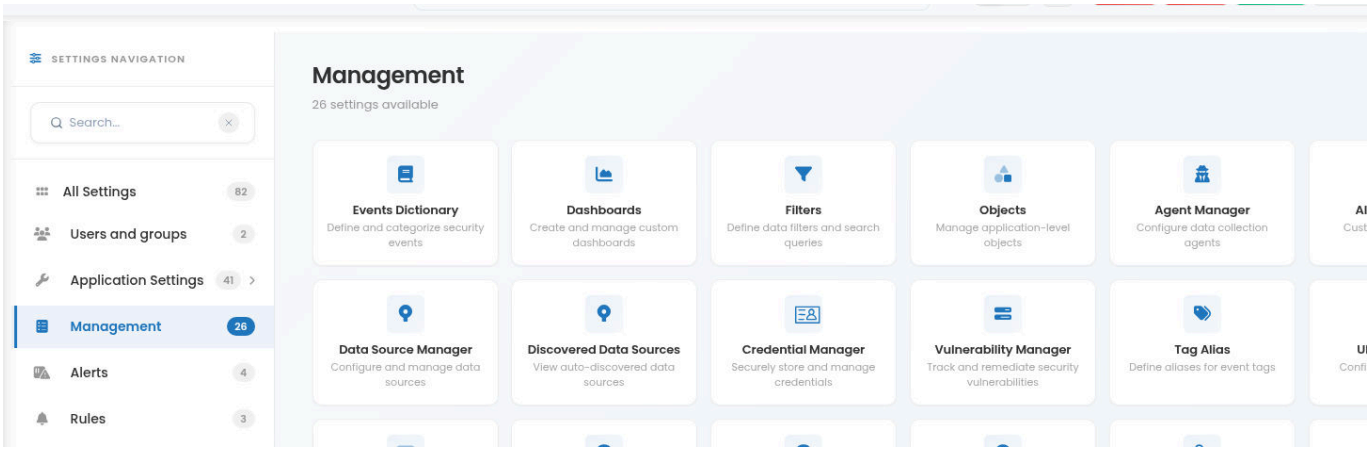
In order to use Tag Alias you have to identify the Initial Tag in the Browser Module. Initial Tag could have: EventID 100000, another initial tag which doesn't exist in Data Acquisition or without data on STRINGFIELDS.

To access this function you have to open Tag alias page following the steps bellow:

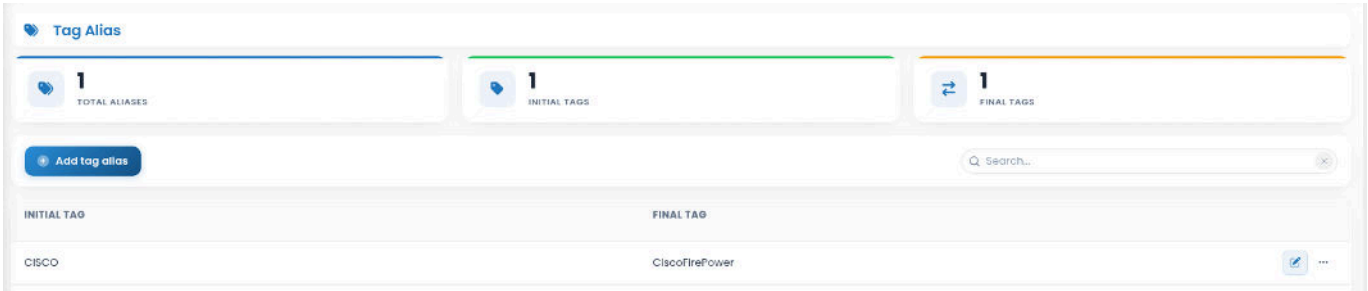
a) Navigate to Settings



in the left side of the interface where are the quick access buttons, then click **Management > Tag Alias**:



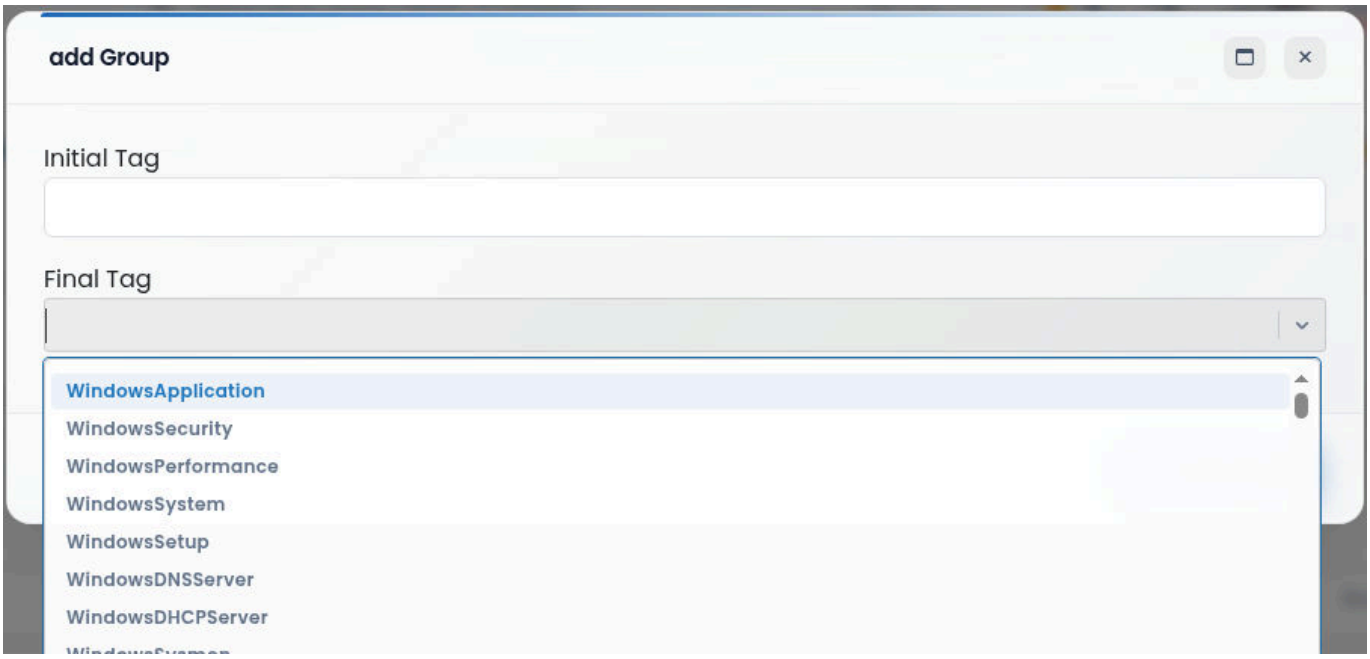
b) Tag Alias window will open:



To add a new Tag Alias that you found in Browser Module, press



button and the window will open:



Complete the following:

- **Initial Tag**: the Tag which you found in Browser Module that is not processed in CYBERQUEST.
- **Final Tag**: you can choose from the predefined list the data sources tag. The events will be processed with the used Final Tag.

Edit



button on the right corner allows you to edit selected group.

To delete a group from the list, press

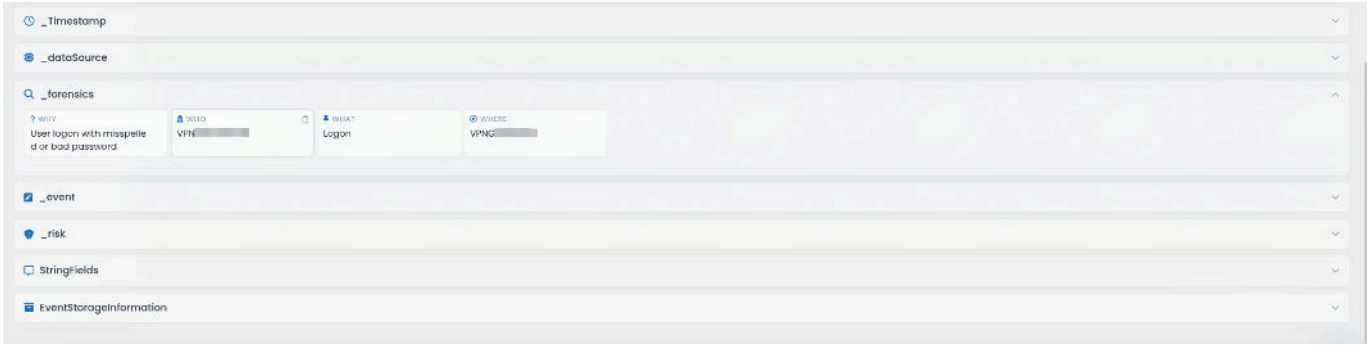
button next to it and select **Delete**. As a measure of precaution, you will be asked to confirm deletion.

Enhanced parsing

Enhance parsing is translating events and adding additional information to what Windows already provides. Windows Events Enricher adds the following information on the Forensics field:

- **Who** - describes who created the event
- **What** - the Category of the event
- **Where** - describes the location where the event occurred
- **Why** - describes why the event was created

For example, go to **Browser Module** and search the **EventID: 4625** and you will find the category field which is named **_FORENSICS**. There you will see 4 forencsics fields of Windows Enricher:



- **Who**: “UserName/Account Name”
- **What**: “Category”
- **Where**: “Computer”
- **Why**: ""

Supported DataSources

CYBERQUEST is an innovative Big Data Security Analytics Platform designed to provide total auditing and security coverage for your enterprise network.

CYBERQUEST collects and correlates data from the entire infrastructure, from existing SIEM systems, business applications and other security tools, such as vulnerability management solutions, IDS /IPS, Data Loss Prevention tools, Firewalls, as follows:

Source of log	Data Sources
**Operating Systems **	
Windows based OS	Microsoft Hyper-V
Unix based	vmware HUAWEI
Linux	Linux
Networking	
Manage Switches	CISCO hp
Routers	CISCO
Firewalls	JUNIPER NETWORKS SONICWALL FORTINET CHECK POINT CISCO Forcepoint
WiFi	NETGEAR
Security devices	
MISC	
NetFlow	
SNMP Traps	NMPv1, SNMPv2c and SNMPv3. Passive collection of SNMP Trap messages, with a library of 388 MIB files available for processing and interpreting received traps.
Applications	

Source of log	Data Sources
Cloud	  
On prem	         
PrintService	
Databases	 
Threat Intelligence	

Data Scanner

Data Sources - Data Scanner

Besides passive collection, in which CYBERQUEST receives messages sent by the source, the platform also performs **active collection**: it queries the devices and applications directly, at configurable intervals, using standard protocols. This collection method is agentless — no software component is installed on the queried device.

Active collection is configured from the web interface, in the **Data Scanner** module. For the configuration procedure, refer to Data Scanner.

Supported protocols

Protocol	Transport	Applicability	Collected information
SNMP	UDP 161	Network equipment, servers with an SNMP agent	Device classification, performance metrics, configuration inventory, routing state
SSH	TCP 22	Unix and Linux systems, network equipment	Host metrics, running processes, device configuration, service availability
WMI	DCOM / MSRPC	Windows systems	Host metrics, running processes
Telnet	TCP 23	Network equipment	Device configuration, service availability
JDBC	database port	Database instances	Availability and database metrics
JMX	HTTP / Jolokia	Java applications	JVM and application metrics
VM SDK	HTTPS	VMware vSphere infrastructure	Host and virtual machine inventory
ICMP	—	Any addressable device	Reachability
DNS	UDP/TCP 53	Name servers	Service availability
HTTP, HTTPS	TCP 80, 443	Web applications and services	Service availability
LDAP	TCP 389	Directory services	Service availability
SMTP, IMAP, POP3, POP3S	TCP 25, 143, 110, 995	Mail services	Service availability
FTP	TCP 21	File transfer services	Service availability
SCP	TCP 22 (SSH)	File transfer services	Service availability

SNMP is supported in versions v2c and v3. For v3, authentication and encryption are performed with the credentials stored in the platform credential store.

Types of collected information

Active collection produces four categories of information, each of which can be used in searches, reports, and correlation rules alongside the events received through passive collection.

- **Performance** - Utilization metrics of processors, memory, storage, and network interfaces, collected from devices, operating systems, databases, and Java applications. Values are collected at every cycle and form a time series.
- **Availability** - Reachability of monitored devices and services, verified with the protocol of each service — an ICMP echo request, a name resolution, an HTTP request, a mail session, and so on. Each verification records the state and the response time.
- **Configuration change** - Changes to the running configuration of network equipment, detected by comparing the fingerprint of the current configuration with the previously stored version. A change is reported only when the configuration actually differs, so unmodified equipment produces no events.

- **Routing state** - The state of BGP and OSPF adjacencies, obtained from the neighbor tables of the equipment. A neighbor that leaves its established state is reported.

Devices discovered through queries also produce a fifth category, the **configuration inventory** described below, which populates the local device database rather than the event stream.

Collected metrics

The metrics available for a device depend on the protocol through which it is queried:

Protocol	Metrics
SNMP	Processor load, memory used, uptime, number of interfaces, number of interfaces in the up state
WMI	Processor load, number of logical processors, total and free memory, total and free disk space, total and running services
JDBC	Number of rows returned by the configured query, and every numeric column of its result

Collection is best-effort: a value that the queried device does not expose is omitted from that cycle without failing the collection. Metrics can be charted per device and used as the condition of an alerting rule — refer to Data Scanner.

Where the collected information appears

Information	Where to find it
Performance metrics	**Settings > Application Settings > Data Scanner > Devices**, through the metrics action of a device
Availability, current state and uptime	**Settings > Application Settings > Data Scanner > Availability**
Configuration versions and differences	**Settings > Application Settings > Data Scanner > Config**
Configuration inventory of the equipment	**Settings > Application Settings > Data Scanner > Devices**
All of the above, as events	The **Browser** module, filtering on the event codes below

The information collected actively is normalized into the same event model as the data received passively, so it can be searched in the **Browser** module and used in reports and correlation rules. The event codes are:

Event code	Content
700001	Performance metrics
700002	Availability of a service
700003	BGP or OSPF neighbor state
700004	Configuration change on a device
700005	Device classification

Configuration inventory (CMDB)

The information obtained through queries is normalized into a vendor-independent data model and stored in a local configuration database. The database is updated at every collection cycle and reflects the current state of the equipment fleet.

For each discovered device, the platform maintains:

Information	Standard object queried
Operating system, firmware	`sysDescr` (SNMPv2-MIB); SSH; WMI
Device serial number	`entPhysicalSerialNum` (ENTITY-MIB)
Interface name	`ifDescr` (IF-MIB)
IP address and subnet mask	`ipAdEntAddr`, `ipAdEntNetMask`, `ipAdEntIfIndex` (IP-MIB)
Interface status	`ifAdminStatus`, `ifOperStatus` (IF-MIB)
Transmission speed	`ifSpeed` (IF-MIB)
MAC address	`ifPhysAddress` (IF-MIB)
Running processes	`hrSWRunTable` (HOST-RESOURCES-MIB); SSH; `Win32_Process` (WMI)

The inventory of a device can be consolidated from several protocols. A device queried both through SNMP and through SSH has a single entry in the database, and each collected item remains traceable to the protocol through which it was obtained.

The inventory is listed in the web interface, in the **Data Scanner** module, in the **Devices** section. Refer to Data Scanner.

Automatic classification

Devices discovered through queries are classified automatically, without operator intervention, based on the identifiers reported by the device. Classification determines the manufacturer, the product family, and the device category — network equipment, server, workstation, or application.

Classification is performed against a corpus of standard and manufacturer-specific MIB definitions included in the platform, which is used to resolve object identifiers and enterprise numbers reported over SNMP.

Credentials

The credentials used for querying are stored in the platform credential store, in encrypted form, and are referenced by the collection targets. They are never displayed in clear text in the interface and are not written into logs.

The operations performed on the queried devices are limited to reading. For device configuration retrieval, only the command that displays the running configuration is executed, selected according to the manufacturer of the device.

Operating Systems

Data Sources - Operating Systems

Source of log	LogName	TagName	Technology	Configuration
Windows OS based				
	Application	`Tag:"WindowsApplication"`	WindowsOs	
	Security	`Tag:"WindowsSecurity"`	WindowsOs	
	System	`Tag:"WindowsSystem"`	WindowsOs	
	DNS Server	`Tag:"WindowsDNSServer"`	WindowsOs	
	Setup	`Tag:"WindowsSetup"`	WindowsOs	
	Microsoft-Windows PrintService/Operational	`Tag:"WindowsPrintService"`	WindowsOs	Print Service
	Microsoft-Windows Backup/Operational	`Tag:"WindowsBackupService"`	WindowsOs	
	Microsoft-Windows Hyper-V Compute/ Operational	`Tag:"HyperVComputeOperational"`	WindowsOs	
	Microsoft-Windows Hyper-V Compute/Admin	`Tag:"HyperVComputeAdmin"`	WindowsOs	
	Microsoft-Windows Hyper-V-Hypervisor/Operational	`Tag:"HyperVHypervisorOperational"`	WindowsOs	
	Microsoft-Windows Hyper-V-Hypervisor/Admin	`Tag:"HyperVHypervisorAdmin"`	WindowsOs	
	Microsoft-Windows Hyper-V-VMMS/Admin	`Tag:"HyperVVMMSAdmin"`	WindowsOs	

Source of log	LogName	TagName	Technology	Configuration
	Microsoft-Windows Hyper-V-VMMS/Networking	`Tag:"HyperVVMMSNetworking"`	WindowsOs	
	Microsoft-Windows Hyper-V-VMMS/Operational	`Tag:"HyperVVMMSOperational"`	WindowsOs	
	Microsoft-Windows Hyper-V-VMMS/Storage	`Tag:"HyperVVMMSStorage"`	WindowsOs	
	Microsoft-Windows Hyper-V-VmSwitch/Operational	`Tag:"HyperVVmSwitchOperational"`	WindowsOs	
	Microsoft-Windows Hyper-V-Worker/Admin	`Tag:"HyperVWorkerAdmin"`	WindowsOs	
	Microsoft-Windows Hyper-V-Worker/Operational	`Tag:"HyperVWorkerOperational"`	WindowsOs	
	Windows Print Service	`Tag:"WindowsPrint"`	Syslog	
	Microsoft Windows Security Windows File Audit	`Tag:"CQWindowsFileAudit"`	Syslog	
Unix based				
	HuaweiEulerOS	`Tag:"HuaweiEulerOS"`	Syslog	
	VmWareVCSA	`Tag:"VmWareVCSAParser"`	Syslog	
	Firmware update manager client utility	`Tag:"CQfwupdmgr"`	Syslog	
Linux				
	SyslogTCP	`Tag:"SyslogTCP"`	Syslog	
	SyslogUDP	`Tag:"SyslogUDP"`	Syslog	

Source of log	LogName	TagName	Technology	Configuration
	GenericDebian	`Tag:"GenericDebian"`	Syslog	
	GenericCentOS	`Tag:"GenericCentOS"`	Syslog	
	audispd	`Tag:"CQaudispd"`	Syslog	
	sudo	`Tag:"CQsudo"`	Syslog	
	su	`Tag:"CQsu"`	Syslog	
	sshd	`Tag:"CQsshd"`	Syslog	
	chfn	`Tag:"CQchfn"`	Syslog	
	groupadd	`Tag:"CQgroupadd"`	Syslog	
	useradd	`Tag:"CQuseradd"`	Syslog	
	userdel	`Tag:"CQuserdel"`	Syslog	
	passwd	`Tag:"CQpasswd"`	Syslog	
	CRON	`Tag:"CQCRON"`	Syslog	
	crontab	`Tag:"CQcrontab"`	Syslog	
	MariaDB	`Tag:"CQmariadb"`	Syslog	MariaDBAudit
	systemd	`Tag:"CQsystemd"`	Syslog	
	systemd-timesyncd	`Tag:"CQsystemd-timesyncd"`	Syslog	

Source of log	LogName	TagName	Technology	Configuration
	dhclient	`Tag:"CQdhclient"`	Syslog	
	dockerd	`Tag:"CQdockerd"`	Syslog	
	Linux multipathd service	`Tag:"CQmultipathd"`	Syslog	
	Rng-tools	`Tag:"CQrngd"`	Syslog	
	Generic Linux	`Tag:"GenericLinux"`	Syslog	Linux
	Linux Logrotate	`Tag:"CQlogrotate"`	Syslog	
	Linux user modification logs	`Tag:"CQusermod"`	Syslog	
	Systemd Login Manager	`Tag:"CQsyswrapper"`	Syslog	
	Linux fstrim logs	`Tag:"CQfstrim"`	Syslog	

Networking

Data Sources - **Networking**

Source of log	LogName	TagName	Technology	Configuration
Managed Switches				
	HPSwitch	`Tag:"HPSwitch"`	Syslog	
	CiscoSwitch	`Tag:"CiscoSwitch"`	Syslog	
	Unify Switch	`Tag:"CQswitch"`	Syslog	
	FortiSwitch	`Tag:“FortiSwitch”`	Syslog	
Routers				
	CQCiscoMeraki	`Tag:"CQCiscoMeraki"`	Syslog	
	Keepalived Virtual Router Redundancy Protocol Daemon	`Tag:"CQKeepalived_vrrp"`	Syslog	
Firewalls				
	CiscoASA	`Tag:"CiscoASA"`	Syslog	
	CheckPointFirewall	`Tag:"CheckPointFirewall"`	Syslog	
	FortinetFortiGate	`Tag:"FortinetFortiGate"`	Syslog	Fortinet FortiGate
	FortinetFortyWeb	`Tag:"FortinetFortyWeb"`	Syslog	
	ImpervaWAF	`Tag:"ImpervaWAF"`	Syslog	

Source of log	LogName	TagName	Technology	Configuration
	Juniper	`Tag:"Juniper"`	Syslog	
	StormShieldFirewall	`Tag:"StormShieldFirewall"`	Syslog	
	SonicWallCEF	`Tag:"SonicWallCEF"`	Syslog	
	ForcePointCEF	`Tag:"CQForcePointCEF"`	Syslog	
	SonicWallFirewall	`Tag:"SonicWallFirewall"`	Syslog	
	pfSense Firewall	`Tag:"PFSenseFirewall"`	Syslog	
	ForcePoint CEF	`Tag:"ForcePointCEF"`	Syslog	
	Palo Alto FW	`Tag:"PaloAltoFW"`	Syslog	
	FortiNet Web application firewall	`Tag:"FortiWaf"`	Syslog	
	Fortinet Forti Web	`Tag:"FortinetFortiWeb"`	Syslog	
	Endian Firewall	`Tag:"EndianFirewall"`	Syslog	
WiFi				
	NetGearAP	`Tag:"NetGearAP"`	Syslog	NetGear AP
Security devices				
	FortiAnalyzer	`Tag:"FortiAnalyzer"`	Syslog	

Source of log	LogName	TagName	Technology	Configuration
	FortiManager	`Tag:"FortiManager"`	Syslog	
	FortiAuthenticator	`Tag:"FortiAuthenticator"`	Syslog	
MISC				
NetFlow				
	NetFlow	`Tag:"NetFLow"`	Syslog	
	NetFlow	`Tag:"NetFLow"`	NetFlow	
	CQ NetFlow DataSource coming from network Devices	`Tag:"CQnetflow"`	Syslog	

Applications

Data Sources - **Applications**

Source of log	LogName	TagName	Technology	Configuration
Cloud				
	AWSCloudTrail	`Tag:"AWSCloudTrail"`	Syslog	
	Office365 Exchange	`Tag:"Office365"`	CQApi	
	Office365 SharePoint	`Tag:"Office365"`	CQApi	
	Office365 AzureActiveDirectory	`Tag:"Office365"`	CQApi	
	Change Auditor for Azure AD	`Tag:"ChangeAuditorAzureActiveDirectory"`	Applications	
	cloudera_HDFS_AUDIT	`Tag:"cloudera_HDFS_AUDIT"`	Applications	
	cloudera_HBASE_AUDIT	`Tag:"cloudera_HBASE_AUDIT"`	Applications	
	cloudera_HIVE_AUDIT	`Tag:"cloudera_HIVE_AUDIT"`	Applications	
	cloudera_HUE_AUDIT	`Tag:"cloudera_HUE_AUDIT"`	Applications	
	cloudera_NAVMS_AUDIT	`Tag:"cloudera_NAVMS_AUDIT"`	Applications	
	cloudera_SENTRY_AUDIT	`Tag:"cloudera_SENTRY_AUDIT"`	Applications	

Source of log	LogName	TagName	Technology	Configuration
	cloudera_SOLR_AUDIT	`Tag:"cloudera_SOLR_AUDIT"`	Applications	
	cloudera_IMPALA_AUDIT	`Tag:"cloudera_IMPALA_AUDIT"`	Applications	
	Cloud GravityZone	`Tag:"CloudGravityZone"`	Syslog	
On Prem Antimalware				
	BDGravityZone	`Tag:"BDGravityZone"`	Syslog	Bitdefender Gravity Zone
	McAfeeSplit	`Tag:"McAfeeSplit"`	Syslog	
	SymantecServer	`Tag:"CQSymantecServer"`	Syslog	
	EsetAntivirus	`Tag:"EsetAntivirus"`	Syslog	
	ESET PROTECT Center	`Tag:"EsetProtectCenter"`	Syslog	
On prem Application servers				
	Veeam Agent	`Tag:"WindowsVeeamAgent"`	WindowsOs	
	Microsoft-IIS-Logging/Logs	`Tag:"WindowsIISEventLog"`	WindowsOs	
	WSO2	`Tag:"CQwso2is"`	Syslog	WSO2
	IBM-SAN	`Tag:"IBM-SAN"`	Syslog	

Source of log	LogName	TagName	Technology	Configuration
	SynologyFTP-NAS	`Tag:"SynologyFTP-NAS"`	Syslog	
	Dovecot	`Tag:"CQdovecot"`	Syslog	
	MailPostfix	`Tag:"MailPostfix"`	Syslog	
	ApacheDatasource	`Tag:"ApacheDatasource"`	Syslog	Apache
	Qnap	`Tag:"Qnap"`	Syslog	
	DMSPortalMapEventType	`Tag:"DMSPortalMapEventType"`	Syslog	
	ITrustSysLog	`Tag:"ITrustSysLog"`	Syslog	
	KiwiSyslog	`Tag:"KiwiSyslog"`	Syslog	
	ElasticSearchSyslog	`Tag:"ElasticSearchSyslog"`	Syslog	
	MSExchange	`Tag:"MSExchange"`	Syslog	
	GitLabRails	`Tag:"GitLabRails"`	Syslog	
	GitLabShell	`Tag:"GitLabShell"`	Syslog	
	InsoftAuditLog	`Tag:"InsoftAuditLog"`	Syslog	

Source of log	LogName	TagName	Technology	Configuration
	DMSPortalMap	`Tag:"DMSPortalMap"`	Syslog	
	DMSPortalApplication	`Tag:"DMSPortalApplication"`	Syslog	
	DMSPortalMapEventType	`Tag:"DMSPortalMapEventType"`	Syslog	
	nginx_combined	`Tag:"CQnginx_combined"`	Syslog	
	apache_combined	`Tag:"CQapache_combined"`	Syslog	
	InTrust for AD	`Tag:"ChangeAuditorInTrustActiveDirectory"`	Applications	
	Elasticsearch	`Tag:"GenericElasticSearch"`	CQApi	
	LogStash	`Tag:"LogStash"`	CQApi	
	CQHttpServer	`Tag:"CQHttpServer"`	CQApi	
	Generic CQ API	`Tag:"GenericCQApi"`	CQApi	
	DekeneasOrangeRo	`Tag:"DekeneasOrangeRo"`	CQApi	
	Generic Files	`Tag:"GenericFile"`	Applications	
	Generic CSV Files	`Tag:"GenericCSVFile"`	Applications	CSVFile

Source of log	LogName	TagName	Technology	Configuration
	Exchange TrackingSource Files	`Tag:"ExchangeMessageTracking"`	Applications	
	Microsoft Exchange Message Tracking	`Tag:"MSExchnangeParser"`	Syslog	
	SendMail Mail Daemon	`Tag:"CQsm-msp-queue"`	Syslog	
	CEF Formatted events (Common Event Format	`Tag:"CQCEF"`	Syslog	
	Subversion Mail	`Tag:"CQsvn"`	Syslog	
	Postfix local mail delivery	`Tag:"CQpostfix/local"`	Syslog	
	Amavis mail service	`Tag:"CQamavis"`	Syslog	
	Named DNS service	`Tag:"CQnamed"`	Syslog	
	Postfix session count and request rate control	`Tag:"CQpostfix/anvil"`	Syslog	
	PostFix Mail Cleanup Daemon	`Tag:"CQpostfix/cleanup"`	Syslog	
	PostFix error/retry mail delivery agent	`Tag:"CQpostfix/error"`	Syslog	
	PostFix LMTP client	`Tag:"CQpostfix/lmtp"`	Syslog	
	PostFix local mail pickup	`Tag:"CQpostfix/pickup"`	Syslog	

Source of log	LogName	TagName	Technology	Configuration
	PostFix delivery to external command	`Tag:"CQpostfix/pipe"`	Syslog	
	Postfix queue manager	`Tag:"CQpostfix/qmgr"`	Syslog	
	Postfix shared connection cache server	`Tag:"CQpostfix/scache"`	Syslog	
	Postfix SMTP client	`Tag:"CQpostfix/smtp"`	Syslog	
	Postfix SMTP server	`Tag:"CQpostfix/smtpd"`	Syslog	
	Postfix Secure SMTP server	`Tag:"CQpostfix/smtps/smtpd"`	Syslog	
	Postfix delivery status reports	`Tag:"CQpostfix/bounce"`	Syslog	
	Pure FTPd Service	`Tag:"CQpure-ftpd"`	Syslog	
	Quest Change Auditor Exchange Logs	`Tag:"QuestChangeAuditorExchange"`	Syslog	
	Quest Change Auditor Active Directory Audit log	`Tag:"QuestChangeAuditorAD"`	Syslog	
	Cisco Prime	`Tag:"CiscoPrime"`	Syslog	
	InTrust Syslog	`Tag:"InTrustSysLog"`	Syslog	

Source of log	LogName	TagName	Technology	Configuration
	VmWare VCSA	`Tag:"VmWareVCSAParser"`	Syslog	VmWare VCSA
	Ngnix Error Log	`Tag:"CQnginx-error"`	Syslog	
	SSH SFTP server	`Tag:"CQsftp-server"`	Syslog	
	Documenta audit log	`Tag:"DocumentaA$AUDIT"`	Syslog	
	DocumentaLog	`Tag:"DocumentaLog"`	Syslog	
	Dynamic Host Configuration Protocol Server	`Tag:"Dhcpd"`	Syslog	
	LXD system container and virtual machine manager logs	`Tag:"CQlxd.activate"`	Syslog	
On prem Applications				
	VMware ESXI Vpxa	`Tag:"CQVpxa"`	Syslog	
	VMware ESXI Hostd	`Tag:"CQHostd"`	Syslog	
	VMware ESXI Smaill-Footprint CIM Broker (SFCB) Intelligent Platform Management Interface (IPMI)	`Tag:"CQsfcb-vmw_ipmi"`	Syslog	
	VMware ESXI HTTP Reverse Proxy	`Tag:"CQRhttpproxy"`	Syslog	
	VMware ESXI HTTP Kernel Syslogs	`Tag:"CQvmkernel"`	Syslog	
	VMware ESXi Hostd Probe	`Tag:"CQhostd-probe"`	Syslog	

Source of log	LogName	TagName	Technology	Configuration
	VMware ESXi Storage Resource Manager	`Tag:"CQstorageRM"`	Syslog	
	VMware ESXi Storage DRS Injector	`Tag:"CQsdrsInjector"`	Syslog	
	VMware ESXi Kernel Warnings	`Tag:"CQvmkwarning"`	Syslog	
	VMware ESXi Auth Daemon Syslogs	`Tag:"CQvmauthd"`	Syslog	
	VMware ESXi Cron Daemon Syslogs	`Tag:"CQcrond"`	Syslog	
	VMware ESXi Backup Syslogs	`Tag:"CQbackup"`	Syslog	
	VMware ESXi Shell Syslogs	`Tag:"CQshell"`	Syslog	
	VMware ESXi Heartbeat Syslogs	`Tag:"CQheartbeat"`	Syslog	
	VMware ESXi Usb arbitrator	`Tag:"CQusbarb"`	Syslog	
	VMware ESXi Tmpwatch	`Tag:"CQtmpwatch"`	Syslog	
	Systemd Temporary Files Syslogs	`Tag:"CQsystemd-tmpfiles"`	Syslog	
	F5 Big-IP	`Tag:"F5BigIPAudit"`	Syslog	
	Cisco Firepower SFIMS	`Tag:"CQSFIMS"`	Syslog	
	Cisco Firepower Health Monitoring Notify	`Tag:"CQHMNOTIFY"`	Syslog	

Source of log	LogName	TagName	Technology	Configuration
	Unify Kernel	`Tag:"CQkernel"`	Syslog	
	Unify Dropbear	`Tag:"CQdropbear"`	Syslog	
	Unify Host access point daemon	`Tag:"CQhostapd"`	Syslog	
	Unify Lightweight Directory Access Protocol CLI	`Tag:"CQlldpcli"`	Syslog	
	Unify Lightweight Directory Access Protocol Daemon	`Tag:"CQlldpd"`	Syslog	
	Unify Procd	`Tag:"CQprocd"`	Syslog	
	Unify Logread	`Tag:"CQlogread"`	Syslog	
	Unify Mca-ctrl	`Tag:"CQmca-ctrl"`	Syslog	
	Unify Mca-monitor	`Tag:"CQmca-monitor"`	Syslog	
	Unify Qos_control.sh	`Tag:"CQqos_control.sh"`	Syslog	
	Unify Stahtd	`Tag:"CQstahtd"`	Syslog	
	Unify Stamgr	`Tag:"CQstamgr"`	Syslog	
	Unify Sysmon	`Tag:"CQsysmon"`	Syslog	
	Unify Syswrapper	`Tag:"CQsyswrapper"`	Syslog	

Source of log	LogName	TagName	Technology	Configuration
	Unify Urandom_seed	`Tag:"CQurandom_seed"`	Syslog	
	Unify Libubnt	`Tag:"CQlibubnt"`	Syslog	
	Unify Wevent	`Tag:"CQwevent"`	Syslog	
	Unify Uplink-monitor	`Tag:"CQuplink-monitor"`	Syslog	
	Unify Utermd	`Tag:"CQutermd"`	Syslog	
	Unify Mcad	`Tag:"CQmcad"`	Syslog	
	Unify Qos_cl.sh	`Tag:"CQqos_cl.sh"`	Syslog	
	Unify Uplink	`Tag:"CQuplink"`	Syslog	
	Standalone LDAP Daemon	`Tag:"CQslapd"`	Syslog	
	Canonical Livepatch Service Syslogs	`Tag:"CQcanonical-livepatch"`	Syslog	
	Python3 logs	`Tag:"CQpython3"`	Syslog	
	VMware Alias Manager and Ticket Service logs	`Tag:"CQVGAuthService"`	Syslog	
On prem Security Applications				
	FortiMail	`Tag:"FortiMail"`	Syslog	
	Safetica DLP	`Tag:"SafeticaDLP"`	Syslog	

Source of log	LogName	TagName	Technology	Configuration
	CiscoISE	`Tag:"CiscoISE"`	Syslog	
	CiscoFirePower	`Tag:"CiscoFirePower"`	Syslog	
	DarkTrace	`Tag:"DarkTrace"`	Syslog	DarkTrace
	FireEyeIPS	`Tag:"FireEyeIPS"`	Syslog	
	HAProxy	`Tag:"HAProxy"`	Syslog	
	CiscoDuoSecurity	`Tag:"CiscoDuoSecurity"`	Syslog	
	TippingPointCEF	`Tag:"TippingPointCEF"`	Syslog	
	CyberQuest_WebAudit	`Tag:"CQCyberQuest_WebAudit"`	Syslog	
	CEF	`Tag:"ArcSightCEF"`	Syslog	
	JSON	`Tag:"JSON"`	Syslog	
	Quest File Access Audit	`Tag:"QuestFileAccessAudit"`	Applications	
	ActiveDirectoryInformation	`Tag:"ActiveDirectoryInformation"`	Applications	Active Directory Information
	CQ HAProxy	`Tag:"CQhaproxy"`	Syslog	

Source of log	LogName	TagName	Technology	Configuration
	CheckPoint Gaia Operation System	`Tag:"CheckPoint GAIA"`	Syslog	CheckPointGAIA
	Cisco Secure Firewall Management Center	`Tag:"CiscoFMC"`	Syslog	
	Squid Web Proxy	`Tag:"CQsquid"`	Syslog	Squid
	ArcSight	`Tag:"Arcsight"`	Syslog	
	SophosUTM	`Tag:"SophosUTM"`	Syslog	
PrintService				

Databases

Data Sources - Databases

Source of log	LogName	TagName	Technology	Configuration
Databases				
	Oracle 11 System Audit Log	`Tag:"Oracle11AuditLog"`	Databases	Oracle Audit Logs
	Oracle 12 System Audit Log	`Tag:"Oracle12AuditLog"`	Databases	Oracle Audit Logs
	MISP DB Threat information	`Tag:"MispDatabase"`	Databases	
	PostgresSQL Audit Log	`Tag:"SimTAX"`	Databases	Enable PostgreSQL auditing
	PostgresSQL	`Tag:"PostgreSQL"`	Databases	Collect from a PostgreSQL database
	DocumentaClient_dms.flux	`Tag:"PostgreSQL"`	Databases	
	DocumentaClient_dms.$audit	`Tag:"PostgreSQL"`	Databases	
	DocumentaClient_dms.flux_pas	`Tag:"PostgreSQL"`	Databases	
	DocumentaClient_dms.log	`Tag:"PostgreSQL"`	Databases	
	Generic Oracle Database	`Tag:"GenericOracleDatabase"`	Databases	Configure ODBC client for Oracle DB instances
	DMSClientFlux	`Tag:"DMSClientFlux"`	Syslog	
	DMSClientAudit	`Tag:"DMSClientAudit"`	Syslog	

Source of log	LogName	TagName	Technology	Configuration
	DMSClientFluxPas	`Tag:"DMSClientFluxPas"`	Syslog	
	DMSClientLog	`Tag:"DMSClientLog"`	Syslog	
	FogLightAudit	`Tag:"FogLightAudit"`	Applications	
	MSSQL	`Tag:"Generic_MSSQL_Tag"`	Databases	Enable or disable MS SQL Audit
	Sas Viya Cas Audit Log	`Tag:"SasViyaCas"`	Databases	
	CQPostgres	`Tag:"CQpostgres"`	Syslog	Enable PostgreSQL auditing

Threat Intelligence

Data Sources - Threat Intelligence

Source of log	LogName	TagName	Technology	Configuration
Threat Intelligence				
	CQTI	`Tag:"CQThreatIntelligence"`	CQApi	
	NucleonTI	`Tag:"NucleonThreatIntelligence"`	CQApi	
	NucleonActiveThreats	`Tag:"NucleonActiveThreats"`	Syslog	
	MISP			
	Dekeneas		CQApi	

MetaData

MetaData

Source of log	LogName	TagName	Technology	Configuration
	ActiveDirectoryInformation	`Tag:"ActiveDirectoryInformation"`	Applications	Active Directory Information

Vulnerability Scanner

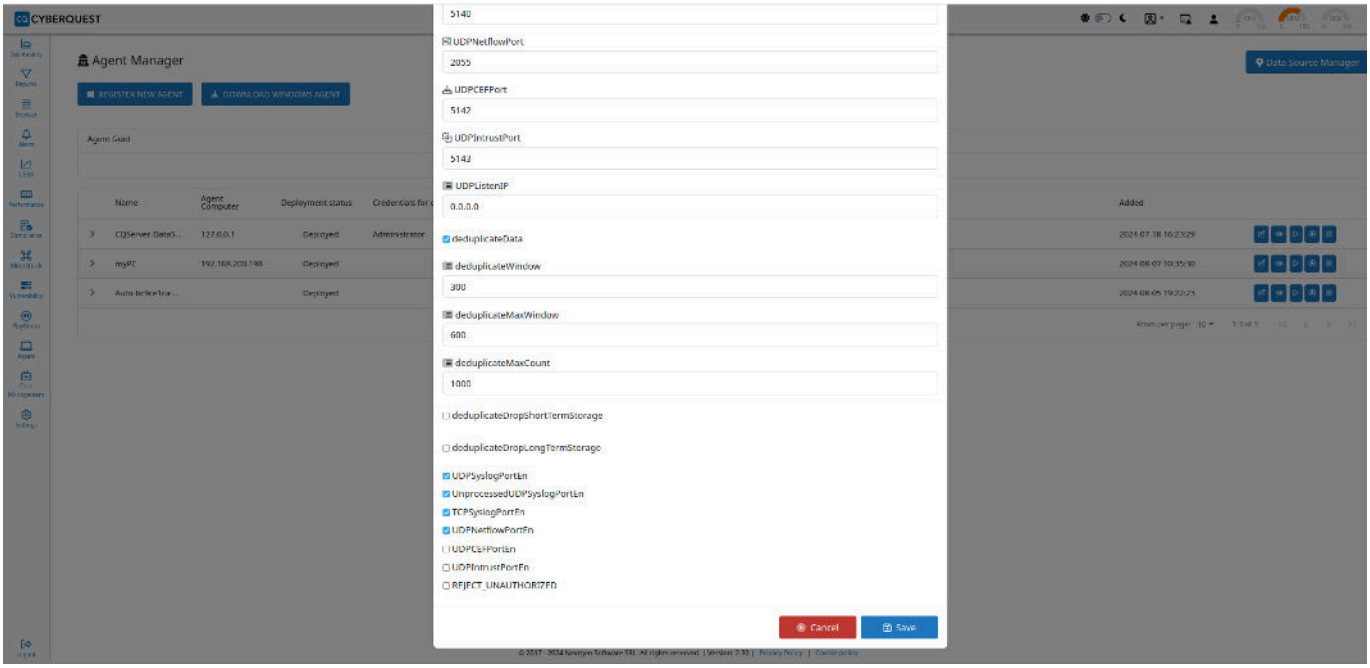
Data Sources - Vulnearbility Scanner

Source of log	LogName	TagName	Technology	Configuration
Vulnerability Scanner				
	Nexpose	`Tag:"Nexpose"`	Syslog	
	openvas-reports	`Tag:"openvas-reports"`	Syslog	
	openvas-assets	`Tag:"openvas-assets"`	Syslog	
	Nessus	`Tag:"nessus-reports"`	CSV	

Data Deduplication

Setting up automated data deduplication in CYBERQUEST is trivial:

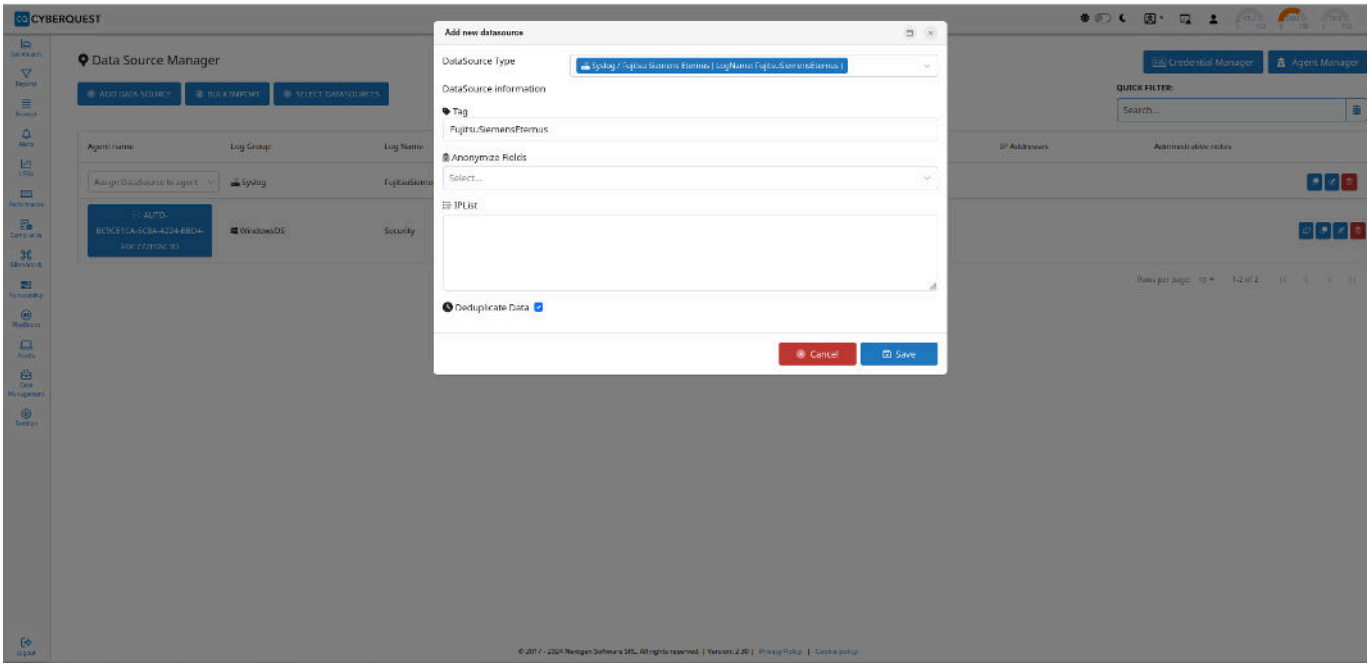
Step 1: Configure Deduplication settings at agent level:



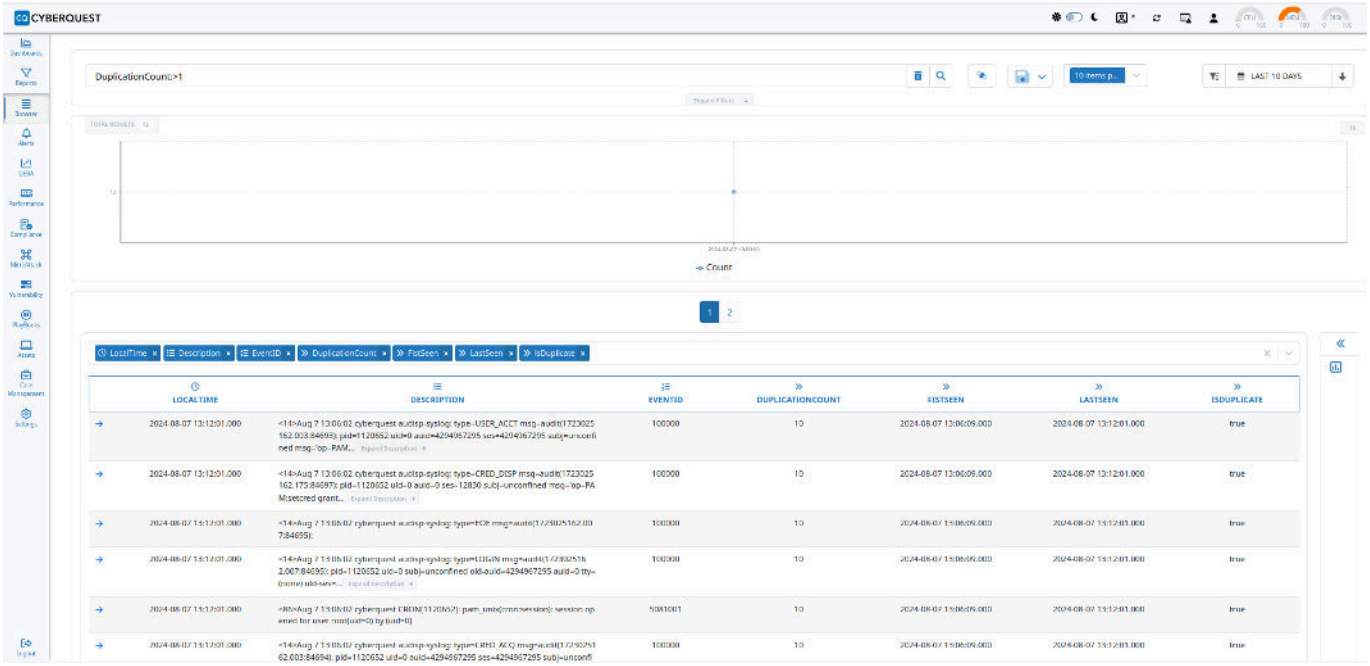
The parameters used for deduplication are:

```
"deduplicateData": false, //does not deduplicate by default
"deduplicateWindow": 300, // expressed in seconds, defines deduplication individual event window
"deduplicateMaxWindow": 600, // expressed in seconds, defines maximum event window
"deduplicateMaxCount": 1000, // expressed in number of maximum event per deduplcated event
"deduplicateDropShortTermStorage": false, // sets duplicate events to be dropped from shortTermDataStorage, by defaul
t false
"deduplicateDropLongTermStorage": false //  sets duplicate events to be dropped from longTermDataStorage
```

Step 2: Configure Deduplication activation at Data Source level



Step 3: Watch for deduplicated events in Browser Module:



FirstSeen - when the first duplicate dataset message appeared;

LastSeen - when the last message in the duplicate dataset appeared;

DuplicateCount - how many times the message was duplicated;

DuplicationHash - this parameter is used to ensure authenticity between messages (it is the element between duplicate messages)

isDuplicate - appears for all messages detected as duplicate, except for the first message (true if the message is duplicate, otherwise false);

isLastDuplicate - true, only on the last duplicate message, false on the rest.

Also, manual data deduplication is possible in order to mark duplicate: Events Manual Deduplication

Web Interface

Introduction

About CYBERQUEST

CYBERQUEST is an innovative Big Data Security Analytics Platform designed to provide total auditing and security coverage for your enterprise network. We have built CYBERQUEST to function as an agile, scalable business platform that intelligently collects and correlates data in the organization's IT infrastructure and works with it to address any type of present or future threat that the business can go through.

CYBERQUEST can be scaled to any organization specific and size, and easily integrates with all security solutions on the market, nomatter of their classification. CYBERQUEST is a true aggregator of security data coming from either security information and event management software, firewalls, intrusion prevention and detection platforms, or email security and endpoint security solutions. In addition, CYBERQUEST can collect, correlate and provide useful insights on heterogeneous data generated by network equipment, servers, databases and applications, which makes it an operational management tool for your administrative and security teams.

Core Capabilities:

- Collect: gather all security and relevant data sources from your IT infrastructure;
- Correlate: add threat intelligence security data for offline or online correlation;
- Detect: quickly identify the most significant threats to your network;
- Visualize: monitor accurately within a single point of access and get specific alerts;
- Respond: Security Orchestration, Automation, and Response (SOAR features) capabilities are embedded in the solution;
- Vulnerability assessment: with OpenVAS integration.

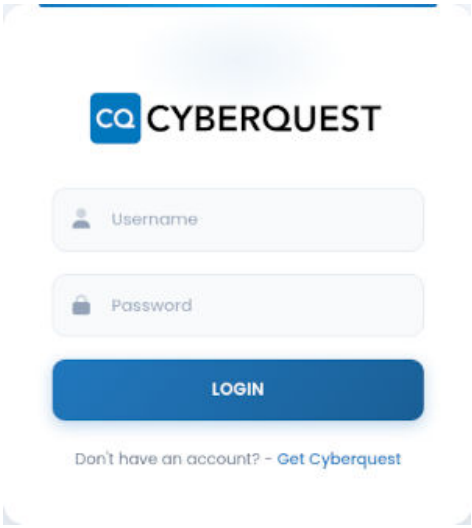
CYBERQUEST aggregates and monitors all activity taking place in your infrastructure and, with real-time alerts, delivers detailed information about vital changes and activities as they occur. Instantly know who, what, where, when, why made a change, and then turn that information into intelligent, in-depth forensics enhanced with additional data from the entire environment, make that information available for auditors and security officers and reduce the risks associated with day-to-day modifications.

Access Web Interface

Web Interface is a consolidated web frontend hosting all administration and operation functionalities of CYBERQUEST. The web interface is compatible with all major browsers on the market.

To access Web Interface, open a web browser and type the application's address or DNS name. The default address initially assigned to Web Interface is ***https://CyberquestIPAddress*** (example).

The browser automatically redirects you to CYBERQUEST's authentication page:



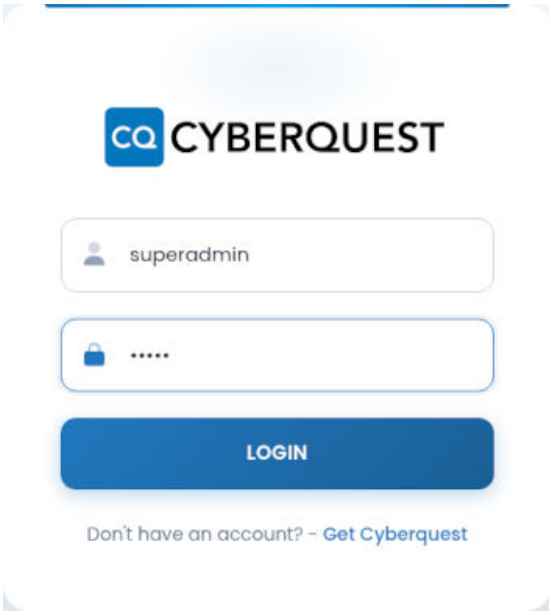
Authentication

User authentication

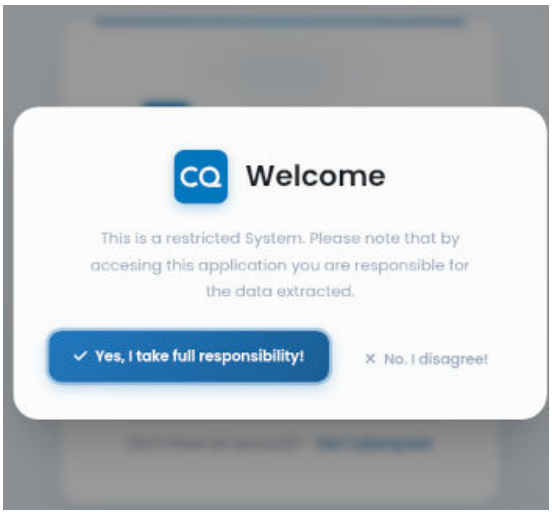
Authentication can be accomplished in one of two ways:

- Using a local user defined in the application;
- Using a company's Active Directory user. This facility allows authentication with Active Directory credentials when LDAP integration has been configured within application. The user must belong to one of two Active Directory security groups: "CYBERQUEST Administrators" or "CYBERQUEST Users".

Type the default username and password, then select the interface language.



You will be prompted with a default message about accessing restricted information. This message is fully customizable.



Accept the responsibility by clicking the button



. Else



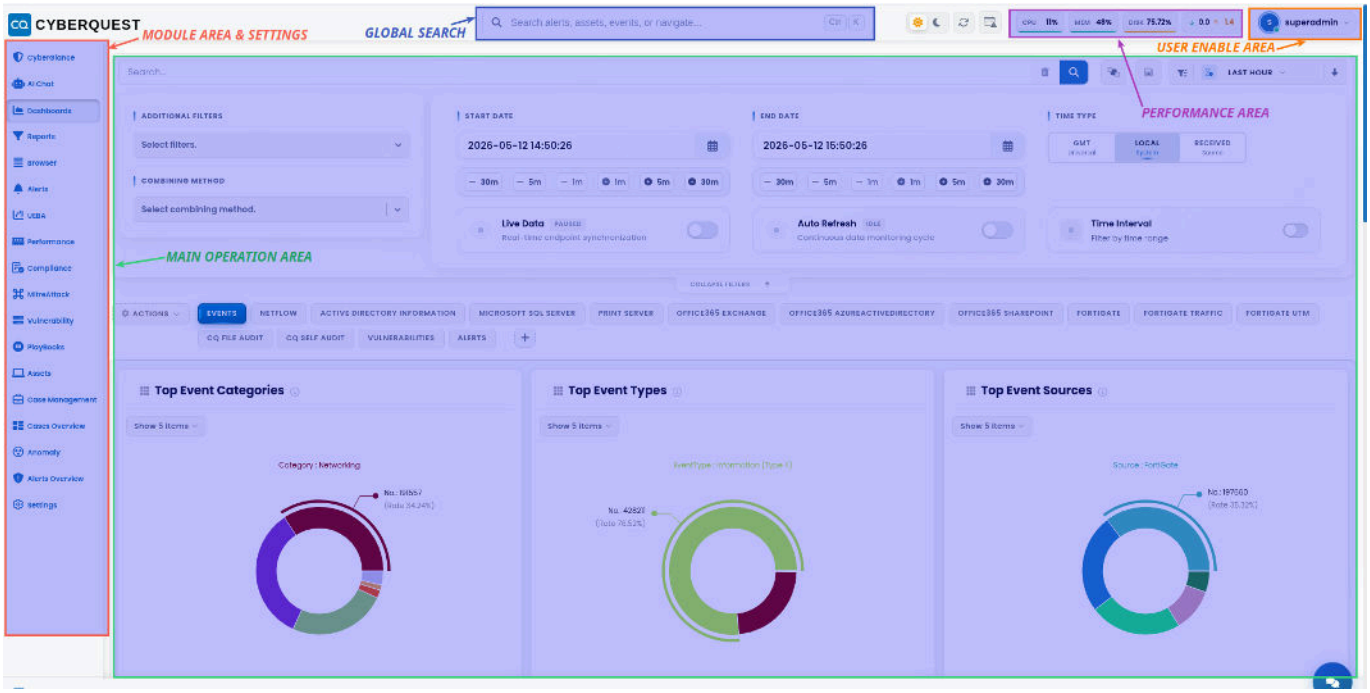
and you will be redirected to the authentication page.

The initial authentication is performed under the default administrative account. When authenticating as administrator, an additional confirmation box is displayed. This additional authentication step was introduced to notify on indiscriminatory access to the entire platform configuration and to require user confirmation of acknowledgement. Superadmin activity should be performed with maximum responsibility and knowledge of platform's administration. Wrongfully changing configuration, rules and retention policies can break access to analytics data, delete or damage objects, and more important, can cause permanently loss of history data.

Web Interface Overview

Once authenticated, CYBERQUEST Web Interface will open. By default, Dashboards module is displayed. Depending on each user's access permissions, the interface may differ. Below we are describing user experience and interface functionalities when authenticating as an administrator.

The Web Interface can be split in several areas:



Module Area

From top-left section of the Web Interface you can select the application module to be displayed in main operation area:

- **Dashboards** is the default module that loads upon initial authentication to the application. It allows operators to quickly view information from the online repository and take action on the graphical objects it contains.
- **Reports** is the application's proprietary reporting module. It includes all predefined and custom reports for general use, as well as reports specific to the authenticated operator.
- **Browser** module is designed to display system log information in a structured and accessible format.
- **Alerts** module is responsible for managing alerts and their correlations. It enables users to initiate comprehensive investigation processes starting from a base alert, which is displayed in the Main Operation Area.
- **Ueba** (User and Entity Behavior Analytics), is a module that enables the analysis of user and entity activity within the enterprise. It helps identify abnormal or potentially malicious behavior by comparing current activity against established baselines, supporting threat detection, insider threat monitoring, and risk assessment.
- **Performance** module displays real-time and historical statistics collected from monitored virtual machines. It provides insights into key performance metrics, including CPU usage history, memory usage history, and storage usage history - specifically for the C: drive. This data helps operators monitor system health, identify performance issues, and optimize resource utilization.
- The **Compliance** module complements the Alerts module by leveraging alerts that are generated and mapped in real time according to the MITRE ATT&CK framework and associated alert tags, which represent standards such as *ISO/IEC 27001:2022, CIS Control V8, GDPR, NIS2, and NIST 800-53*. Using these alerts, the module evaluates the system's compliance with these key regulations. All relevant data is consolidated and displayed within the Compliance module, offering a clear, up-to-date overview of the compliance status.
- The **MITRE ATT&CK** module complements the **Alerts** module by utilizing alerts generated and mapped in real time according to the MITRE ATT&CK framework. Based on these alerts, the module provides a detailed analysis of the tactics and techniques used by potential attackers, facilitating a deeper understanding of threat behaviors. The mapped data is then used to support detection, investigation, and compliance assessment processes. In this way, the MITRE ATT&CK module helps quickly identify attack patterns and improves the efficiency of the security incident response.
- The **Vulnerability** module integrates with OpenVAS, a full-featured vulnerability scanner, to provide comprehensive vulnerability assessment capabilities. It enables the identification, evaluation, and reporting of security weaknesses across the network and systems. By leveraging OpenVAS's extensive database of known vulnerabilities, this module helps organizations proactively detect and address security gaps, enhancing overall risk management and strengthening the security posture.
- CYBERQUEST includes an **automation** module that can be triggered to execute mitigation steps and other actions. These actions can be organized into a "**playbook**," which defines a specific sequence of tasks to effectively carry out mitigation. Playbooks can be easily created, modified, or removed through a graphical interface.

- In the **Assets** module, details are automatically populated as data is collected, ensuring up-to-date information. Additionally, users can manually define new assets or modify existing asset details directly within the system, providing flexible and accurate asset management.
- The **Case Management** module in CYBERQUEST is designed to help organizations create, manage, and track workflows for rapid incident response. Each case has an assigned owner who can involve collaborators to support decision-making and accelerate resolution. The module also allows attaching all relevant evidence related to the triggering event or alert, ensuring a comprehensive and organized investigation process.
- The **Case Overview** module provides a graphical summary of all cases within the organization. It provides an intuitive visual summary of case statuses, priorities, and essential metrics, enabling users to easily monitor progress, manage workloads, and spot potential issues in incident handling.
- The **Anomaly** module detects unusual patterns and behaviors within the system that may indicate security threats or operational issues. By continuously monitoring data and applying advanced analytics, it identifies deviations from normal activity to help organizations proactively uncover potential risks and respond swiftly. This module supports early threat detection and enhances overall situational awareness.
- The **Alerts Overview** module provides a comprehensive graphical summary of alerts, featuring key insights including Riskiest Alerts, Latest Alerts, Status Distribution, Security Score Statistics and Ranges, as well as Top Users, Computers, and Source IPs. This visual dashboard enables quick assessment of alert priorities and trends, supporting efficient monitoring and timely response.

By clicking on



logo displayed in the top-left corner of the Web Interface, you will be taken to the “home” screen that is displayed after logging in to application.

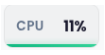
Main Operation Area

The **Main Operation Area** is where users interact with the application to perform their activities. It is tailored to the specific module or mode being accessed, with available options determined by the user’s assigned permissions. Depending on the capabilities of each module, this area can also display personalized content for each user, including custom dashboards and reports.

Available content and options are detailed within each module chapter in *Cyberquest 2.30 User’s Guide*.

Performance Area

Performance Area in the top-right side of the Web Interface maintains three indicators updated in real time:

	**CPU** – displays the current CPU load of the CYBERQUEST Web Application Server. Hovering over the colored section of the graph reveals a tooltip with the exact current load value.
	**Memory** – displays the current memory usage of the CYBERQUEST Web Application Server. Hovering over the colored area of the graph reveals a tooltip showing the exact current load value.
	**Disk** – hows the current disk usage of the CYBERQUEST Web Application Server. Hovering over the colored section of the graph displays a tooltip with the precise current load value.

User Enabler Area

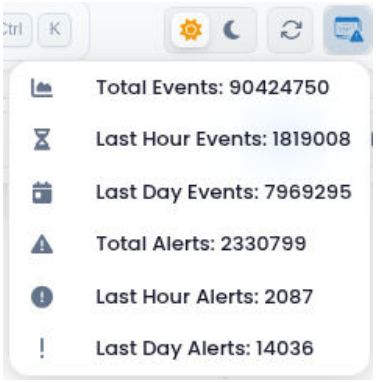
The User Enabler Area, located in the top-right corner of the Web Interface, contains four action buttons:

Events

Press



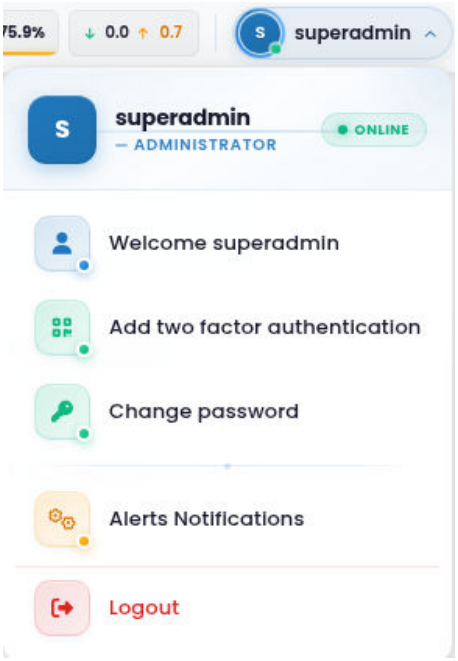
button to open a quick pop-up displaying statistical information about processed data. The following details are provided:



- **Total events** - total number of events currently stored in the online repository
- **Last hour events** - total number of events collected in the last hour
- **Last day events** - total number of events collected in the last day
- **Total alerts** - total number of alerts currently managed by the Application Server
- **Last hour alerts** - total number of alerts raised in the last hour
- **Last day alerts** - total number of alerts raised in the last day

User

Go to ***User actions*** to open the user drop-down menu, which contains the options described below:



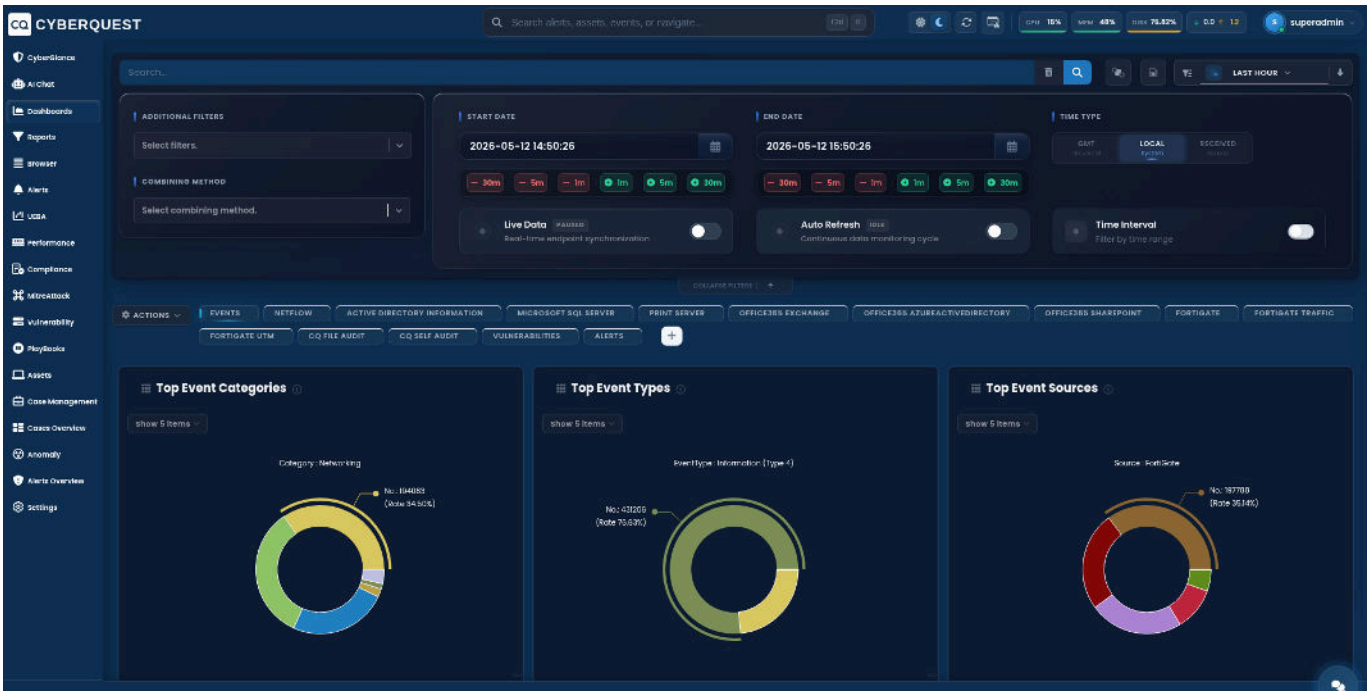
- **Add two factor authentication** - enhances account security by adding an additional verification layer.
- **Change password** opens the Change Your Password window, allowing the currently logged-in user to update their password.
- **Logout** - Logs out the currently logged-in user from the application.
- **Alerts Notifications** provide real-time updates on security alerts. Users can tailor the notifications they receive through configurable filters, ensuring that only relevant and high-priority alerts are displayed based on their preferences or responsibilities.

Dark Mode

Enable dark mode by clicking the



switch located in the top-right corner of the web interface.



Settings

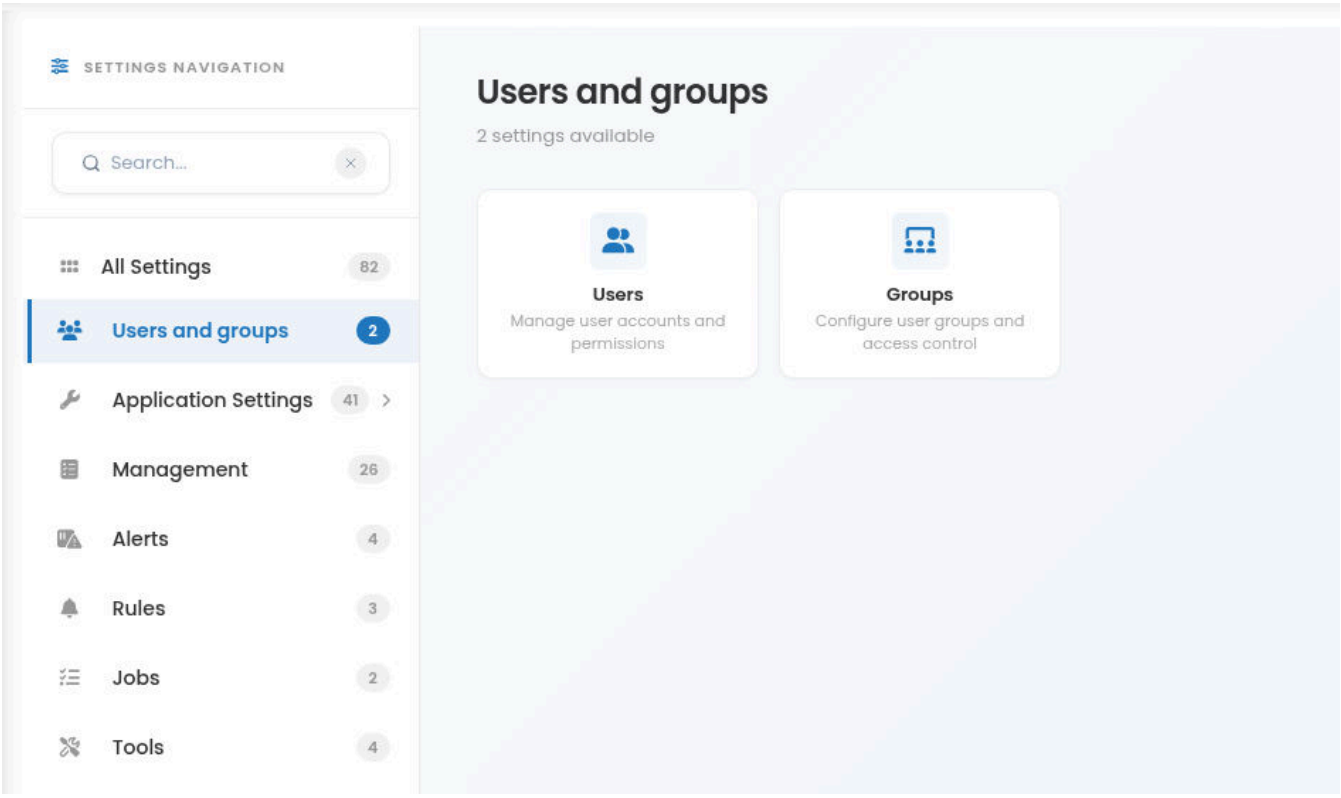
Navigate to **Settings**, by pressing

Settings

button, in the left side of the web interface and the page will open the options described below:

1. **Users and Groups**:

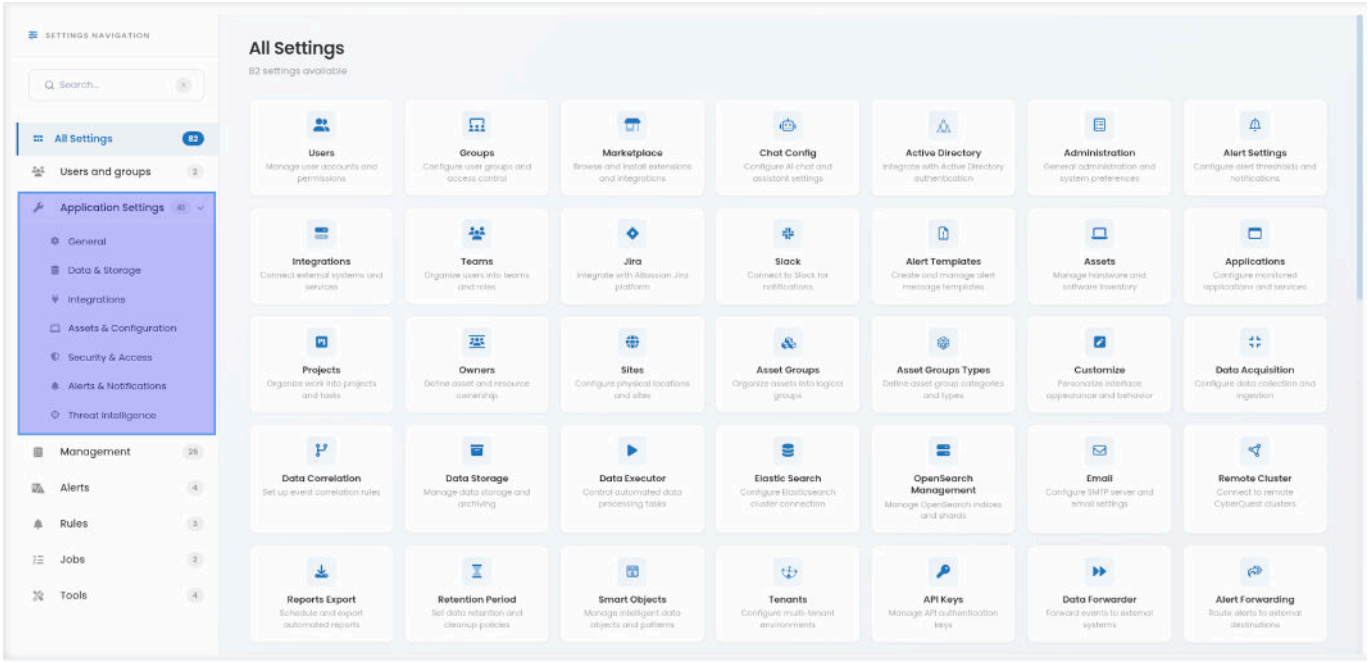
- Users and Groups > **Users**
- Users and Groups > **Groups** - are options allowing an administrator to view, add, edit or delete users and groups. Additional actions are available for users: change password, activate or inactivate, copy dashgroups to users.



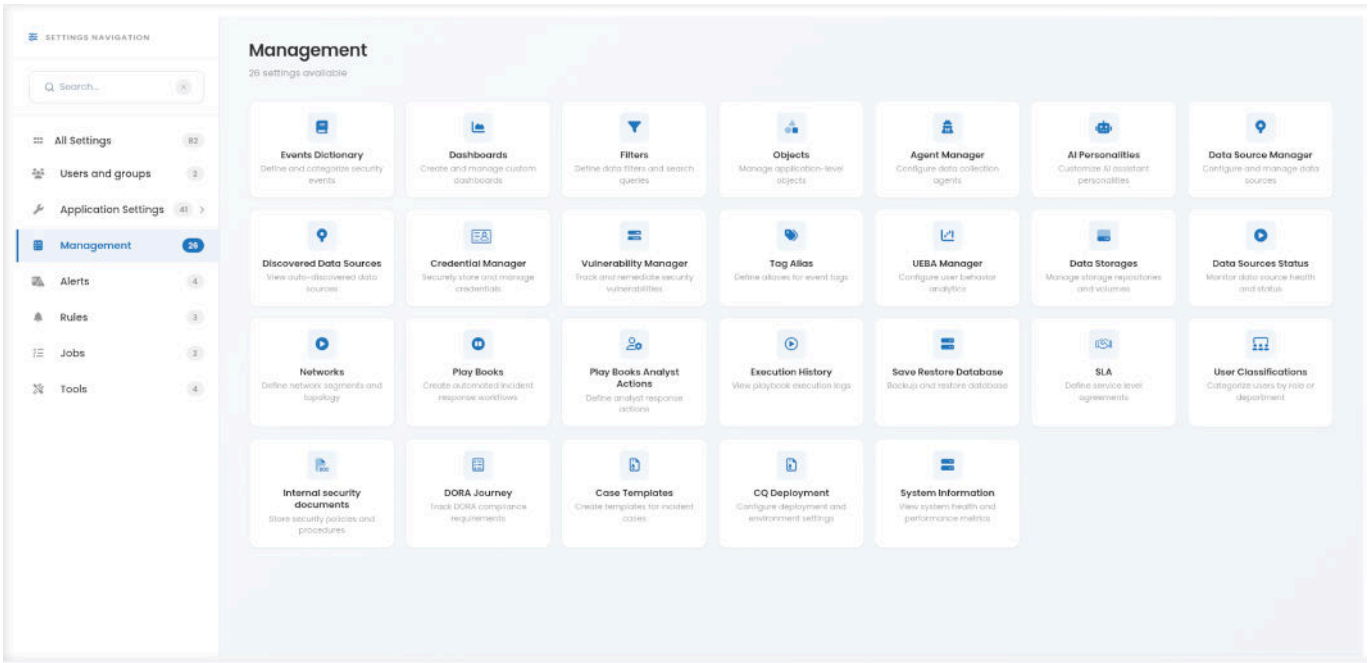
2. **Application Settings**

Each **Application Settings** option opens the *Application Settings* configuration page, allowing administrators to manage and fine-tune the core CYBERQUEST settings. For more details, see the Application Settings

The page presents configuration capabilities for:



3. **Management**



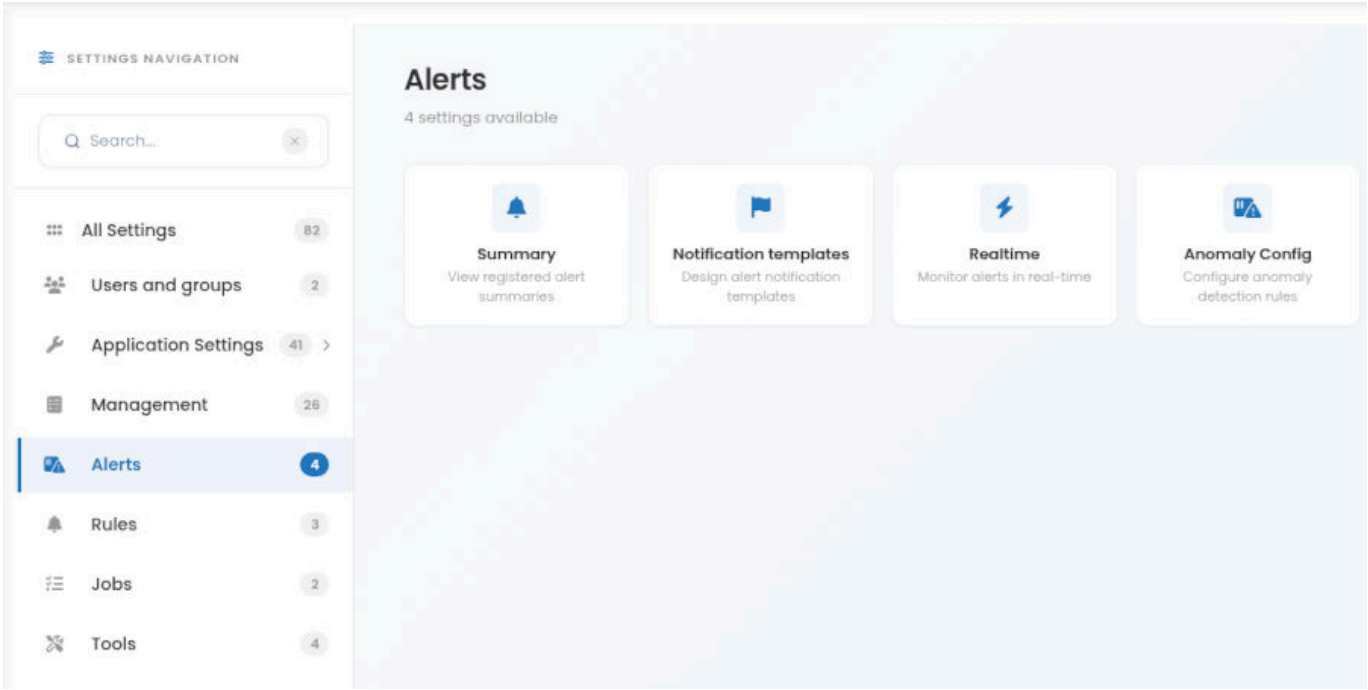
- The **Management > Event Dictionary** option opens the *Event Definitions* configuration page, where an administrator can view all event definitions, create new ones, import definitions from external files, or perform bulk import of objects and update the event dictionary. Available actions on existing entries include exporting, editing, and deleting event definitions.
- The **Management > Dashboards** option opens the *Dashboards* configuration page, where an administrator can view all defined dashboards, import dashboard definitions from external files, and manage existing dashboards with options to edit or delete them.
- The **Management > Filters** option opens the *Filters* configuration page, where an administrator can view all defined filters, create new ones, and manage existing filters with options to edit or delete them.

- The **Management > Objects** option opens the *Object Management* configuration page, where an administrator can view a list of objects or add new ones. Available actions for existing objects include editing and deleting.
- The **Management > AgentManager** option opens the *Agent Manager* configuration page, where an administrator can register new Windows agents. Available actions include editing, deploying, and deleting agents.
- The **Management > AI Personalities** - allows administrators to create, configure, and manage specialized AI personas tailored to different cybersecurity roles, workflows, and operational needs. Each AI Personality can be defined through its identity, scope, capabilities, and tool access, ensuring consistent behavior, role-specific expertise, and controlled interaction within the platform.
- The **Management > DataSourceManager** option opens the *Data Source Manager* configuration page, enabling an administrator to add new data sources.
- The **Management > Discovered Data Sources** option opens the *Discovered Data Sources* page, allowing an administrator to view and manage data sources automatically detected by the system.
- The **Management > CredentialManager** option opens the *Configured Credentials* page, where an administrator can add new credentials and manage existing ones. Available actions include editing and deleting credentials.
- The **Management > VulnerabilityManager** option opens the *Vulnerability Manager* page, where an administrator can update and manage the list of identified vulnerabilities.
- The **Management > Tag Alias** option allows events to be parsed using a custom parser instead of the default one provided by the data server. Available actions include editing and deleting tag aliases.
- The **Management > UEBA Manager** option opens the *UEBA Manager* page, which defines the group membership of users, assets, and events based on their characteristics. Available actions include editing and deleting group configurations.
- The **Management > Data Storages** option opens the *Data Storages* configuration page, where an administrator can create new data storage entries or manage existing ones. Available actions include activating or deactivating, editing, and deleting data storages.
- The **Management > Data Source Status** option opens a report displaying all data sources along with their current status. Administrators can delete data sources, adjust alert timing, and customize the report to include or exclude specific details. The report supports column-based sorting, includes a search field, and can be exported in CSV format for further analysis.
- The **Management > Networks** section allows administrators to configure and organize network segments within the infrastructure. It supports classification by zone and tenant context, enabling more precise monitoring and security scoring. Administrators can verify IP coverage, update network definitions, and manage the lifecycle of each network entry through intuitive actions. Possible actions include checking IP addresses, editing network details, and deleting network entries.
- CYBERQUEST includes an **automation** module that can be triggered to execute mitigation steps and other actions. These actions can be organized into a "**playbook**," which defines a specific sequence of tasks to effectively carry out mitigation. Playbooks can be easily created, modified, or removed through a graphical interface.
- The **Management > PlayBooks Analyst Actions** feature manages analyst interactions during playbook execution. When an Analyst Input or Analyst Confirmation block is reached, the playbook pauses and prompts the analyst with a question. Analysts can view and respond to all active questions in Settings > PlayBooks Analyst Actions to continue the process.
- The **Management > Execution History** page provides detailed logs of each playbook and action execution, essential for debugging and troubleshooting. When errors occur, these logs help identify the root cause, ensuring smooth and error-free playbook operation. Users can view logs directly or download them in .txt format for further analysis.
- The **Management > Save Restore Database** option allows administrators to export the current database for backup purposes and import a database backup to restore system data. These functions help ensure data integrity and facilitate recovery in case of system issues.

- In CYBERQUEST, **Service Level Agreements (SLAs)** are defined based on Case Types to specify confirmation and response time targets for incident and case resolution. These SLAs help ensure timely acknowledgment and resolution of cases according to organizational requirements. After creation, SLAs can be managed through available actions to maintain effective incident handling.
- The **Management > User Classifications** option allows administrators to define and manage categories or classifications for users within the system. These classifications help organize users based on roles, responsibilities, or other criteria, enabling tailored access control, reporting, and analysis across the platform.
- The **Internal Security Documents** function serves as a repository for uploading, exporting, and deleting internal security documents. These documents play a key role in the Dora Journey process, providing essential information and resources used throughout the process.
- The **Management > DORA Journey** function allowing to select internal security documents that serve as evidence for fulfilling the requirements of specific chapters and articles of the DORA Regulation. It integrates with the internal security documents repository to attach relevant materials, and if a document is not found in the repository, it can also be uploaded directly from the local computer. This function helps track the progress of associated actions while verifying that all compliance requirements have been met.
- A **Case Template** offers the ability to build a reusable template used for creating new cases. This template provides the advantage of enabling investigations tailored to the specific needs and processes of the organization. By using case templates, consistency and efficiency are ensured throughout case management, helping standardize workflows and following of internal company documentation.
- The **Management > System Information** - provides a real-time overview of platform health, including active machines, CPU usage, memory consumption, queues, EPS indicators, and last update status.

  It helps administrators quickly monitor system performance, identify resource pressure, and verify that key processing components such as RabbitMQ queues are operating correctly.

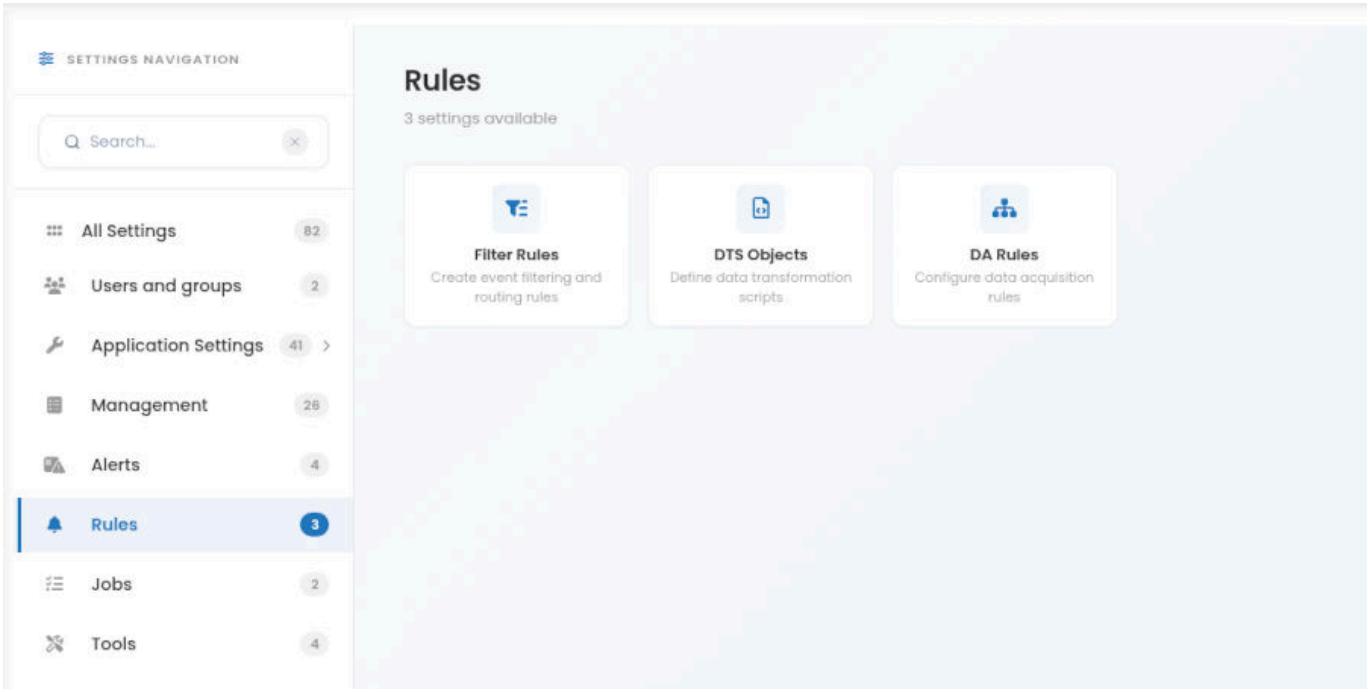
4. **Alerts**



- The **Alerts > Summary** option opens the list of custom summary alerts within the *Alerts* module, allowing administrators to view alert templates, create new alert templates, or add new registered summary alerts. Available actions on existing summary alerts include activate/inactivate, edit, and delete.
- The **Alerts > Notification Templates** option opens the *Alert Templates* configuration page, allowing administrators to create new alert templates or manage existing ones. Available actions on listed templates include edit and delete.

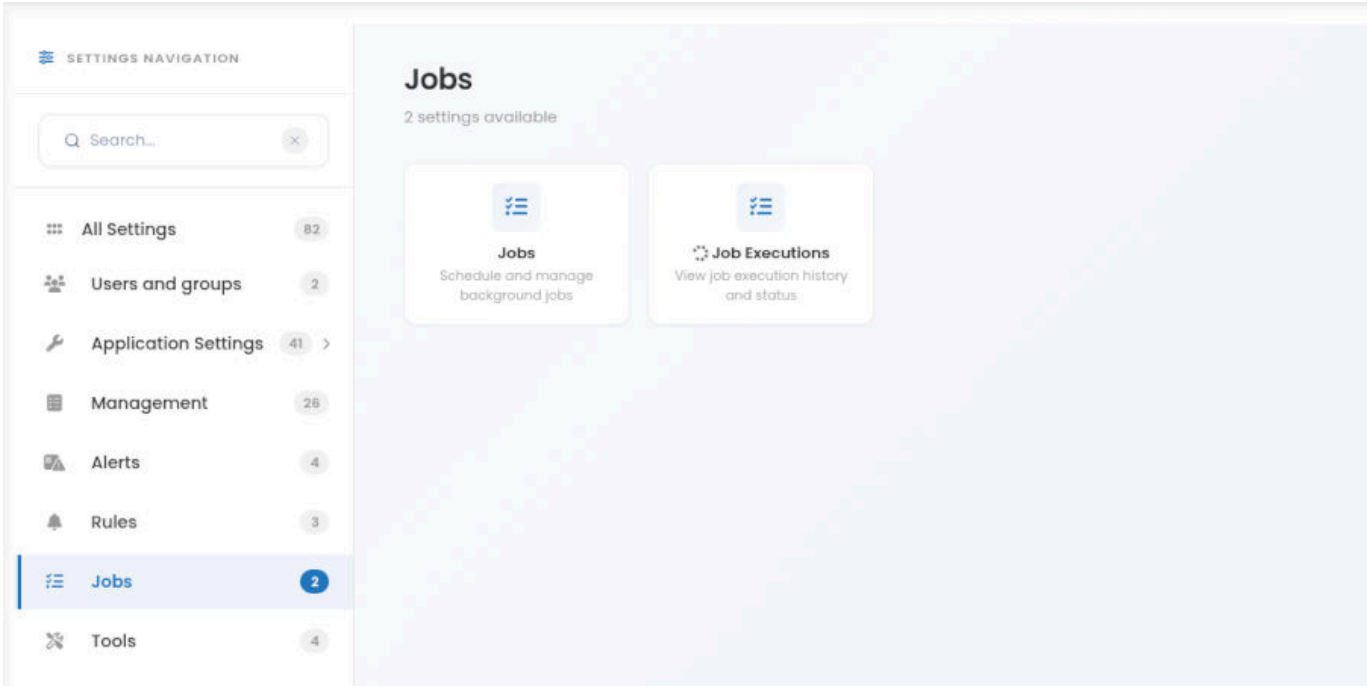
- The **Alerts > Realtime** option opens the list of defined alerts within the *Alerts* module, allowing administrators to create new alert definitions or import alerts from external files. Administrators can also edit, export, clone, or delete existing alert definitions.
- The **Alerts > Anomaly Config** interface allows administrators to define anomaly detection rules based on a report. This configuration enables the system to identify deviations from normal behavior patterns and trigger anomaly alerts accordingly. The module supports customization of detection parameters, offering flexibility in tuning anomaly sensitivity for different use cases.

5. **Rules**



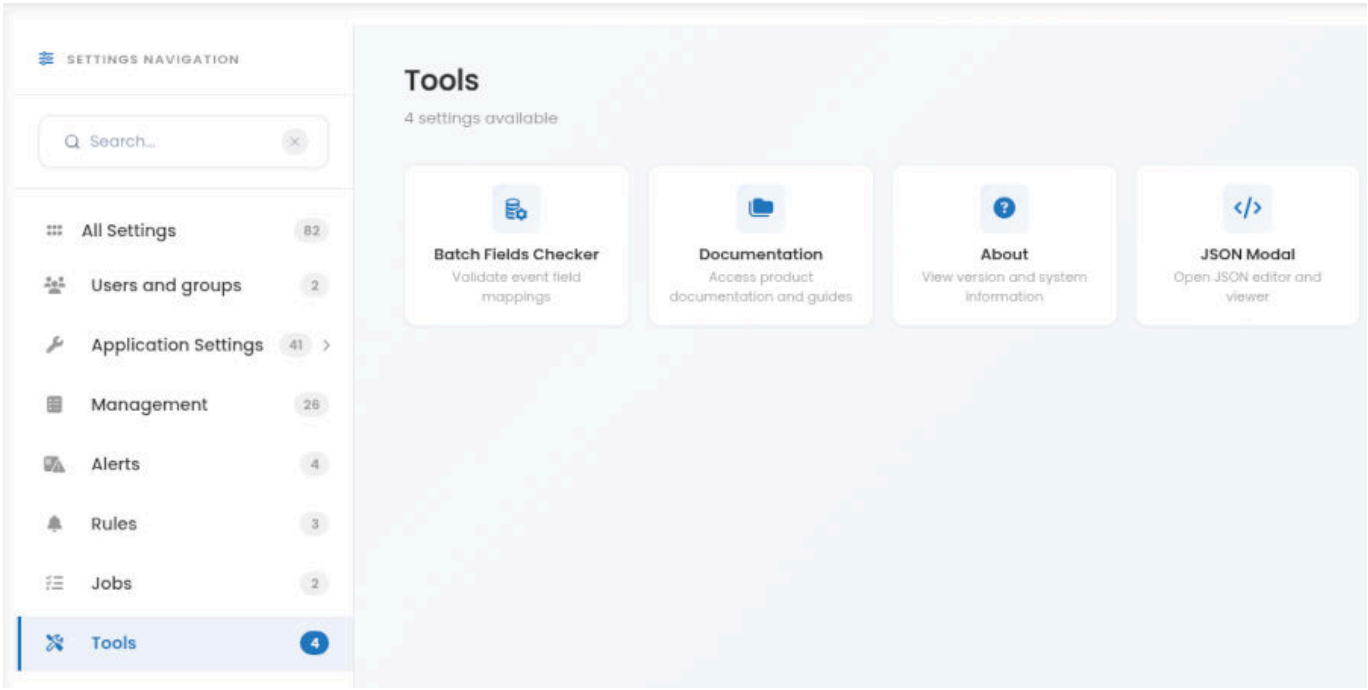
- **Rules > Filter Rules** option opens *Filter Rules* configuration page allowing an administrator to create a new filter rule, import a filter rule from an external file or perform actions on existing ones. Possible actions are activate/inactivate, export, edit and delete.
- **Rules > DTS Objects** option opens *DTS objects* configuration page allowing an administrator to create and import a DTS object from an external file or perform actions on existing ones. Possible actions are activate/inactivate, export, edit and delete.
- **Rules > DA Rules** option opens *DA Rules* configuration page allowing an administrator to create and import a data acquisition rule from an external file or perform actions on existing ones. Possible actions are activate/inactivate, export, edit and delete.

6. **Jobs**



- **Jobs > Jobs** option opens *Jobs* configuration page allowing an administrator to create a new job or perform actions on existing ones. Possible actions are activate/inactivate, run, edit and delete.
- The **Jobs > Jobs Executions** option opens the list of job executions. Job executions can be deleted, and the execution status is displayed for each listed job.

7. **Tools**



- The **Tools > Batch Fields Checker** option opens the *Batch Fields Checker* window, allowing the upload of a text file to execute batch field validation. The results can be exported in CSV format.
- The **Tools > Documentation** option provides a direct link to the technical documentation.
- The **Tools > About** option provides access to system licensing and version information, as well as actions for updating and managing the CYBERQUEST license.
- The **Tools > JSON Modal** option opens a window for viewing and temporarily editing JSON-formatted data.

Using Searches

Running Searches

To begin a search, enter the desired query in the search box. This may include a username, network share path, computer name, or a specific phrase found within event fields.

The search is performed across all available item types - events, users, files, computers, and others -regardless of which item type is currently selected.

To display events from only a specific time period, use the time range filter options in **Search and Filter** section of **Dashboards** or **Browser** modules.

Simple searches return results where the specified term appears anywhere in the discovered data. To narrow the results and increase relevance, search hints can be used by prefixing terms with specific field names. For more details, refer to **Search Term Syntax** below.

Automating Complex Search Scenarios

To begin a search, enter the desired query in the search box—this can be a user name, network share path, computer name, or a phrase to find within event fields.

Certain search workflows are best executed as multi-stage queries, where the results of one search are automatically passed to the next in a sequence. The pipe operator (|) facilitates this process, while field names enclosed in curly braces specify which fields to analyze within the data.

Example 1:

Find the managers of all users who have created or deleted files on the \\FILESRV1\Software network share

```
"\\FILESRV1\Software" OR Description:{SharePath} AND (What="File
Created" OR What="File Deleted") OR Who={Who} OR
DisplayName="{ManagedByDisplayName}"
```

Example 2:

Find events by users from the Milwaukee office on computer FILESRV1

```
Office="Milwaukee" OR Who:{SAMAccountName} AND Where:filesrv1
```

Example 3:

Find computers where members of the Accounting group have logged in

```
"Accounting" OR Who:{SAMAccountName} AND What:logon OR Where={Where}
```

Example 4:

Find all users from the same office as user dshaw

```
Who="dshaw" OR Office="{Office}"
```

Search Term Syntax

Use the following syntax for search terms in the search box. Searches are case-insensitive.

Single-Word Terms

This is known as full-text search. The search involves all available fields and uses the Contains operator.

Meaning	Syntax	Details
Look for a single-word term in any attribute	Word without spaces Example: **john**	**john** matches **John** or **john** in any attribute, but does not match **stjohn** in any attribute
Look for a single-word term with the specified beginning in any attribute	Word ending in an asterisk (*) without spaces Example: **john**	**john*** matches **John** or **Johnson** in any attribute
Find attributes where a specific single word term is not contained in any attributes	Word without spaces with a leading hyphen Example: **-john**	**-john** may match entries that contain **stjohn**, but does not match entries that contain **john** in any attribute
Find entries where a specific single word term with the specified beginning is not contained in any attributes	Word ending in an asterisk (*) without spaces with a leading hyphen Example: **-john** *	**-john*** may match entries that contain **stjohn**, but does not match entries that contain **john** or **johnson** in any attribute
Term Combinations		
Meaning	**Syntax**	**Details**
Look for entries with specific single-word terms in any attributes	Word separated by spaces Example: **john glen***	**john glen*** matches **john** and **glen**, or **john** and **glenda**, or **john** and **glen** and **glenda**, wherever they are found
Look for entries that do not contain specific single-word terms in any attribute	Word without spaces Examples: • **-john -glen** • **John -glen***	• **-john -glen** matches entries that do not contain **john**or **glen** anywhere • **john -glen*** matches entries that contain **john** in any attribute and at the same time do not contain **glen** or **glenda** anywhere
Look for entries with a specific multiple-word phrase in any attribute	Phrase in quotation marks Example: **"Account Logon"**	**"Account Logon"** matches entries that contain the exact phrase **Account Logon** in any attribute
Look for entries that do not contain a specific multiple-word phrase in any attribute	Phrase in quotation marks Example: **logon server01 -"Account Logon"**	**logon server01 -"Account logon"** matches entries that contain the words **Logon** and **server01** anywhere but do not contain the exact phrase **Account Logon** in any attribute
Meet one of the specified terms (or sets of terms)	Terms (single words or phrases) separated by the OR operator; this operator has the following specifics: • it is case-sensitive: it must always be specified as OR • it denotes a choice between everything to the left of it and everything to the right of it • you can use multiple OR operators in a query; the boundary of an OR clause is the beginning of the query, the end of the query, or another OR Examples: • **- paul john OR Thomas** • **-"logon/logoff" server01 OR stjohn**	• **paul john OR Thomas** matches entries that contain either both John and Paul, or Thomas anywhere • **-"logon/logoff" server01 OR stjohn** matches either entries without the phrase **Logon/Logoff** that contains **server01**, or entries with **stjohn** (no matter whether they contain the phrase **Logon/Logoff**)
Explicitly mark an AND operation for visual clarity	Terms (single words or phrases) separated by the AND operator; this operator has the following specifics: • It is case-sensitive: it must always be specified as AND • It can be omitted wherever it occurs Examples: • **Paul AND john** • **Paul john**	**paul AND john** and **paul john** are identical in meaning: look for entries where both **paul** and **john** occur

Meaning	Syntax	Details
Group and nest terms for logical operations on them	Parentheses enclosing the terms you want to group Example: **(homer marge) OR (peter lois)**	**(homer marge OR (peter lois)** matches either entries with both **homer** and **marge**, or entries with both peter and **lois**. It does not match entries with both **peter** and **homer** that do not contain **lois** or **marge**

Searching in Specific Attributes

To apply your search term only to a particular attribute, prepend the name of the attribute with a colon (:) or equals sign (=) to your search term, as shown in the table below. If the attribute name is made up of multiple words, enclose it in brackets (as in [log name]:security). All the syntax conventions described above also apply.

The following distinction is important:

- Labels unambiguously mapped to entry attributes; for example, **Path:"Documents and Settings"** in file access entries. In this case, the search involves the specified field and uses the `Contains` operator.
- Labels mapped to different attributes in different contexts (known as normalized attributes); for example, **Where:primrose** would mean the **primrose** domain for users or groups, the **primrose** computer for files or shares, and so on. In this case, the search involves the associated fields as necessary and may even modify the search terms.

Specifying Quotation Marks

If your search term must include double quotes, then for each double quote you need supply an additional double quote as an escape character. See the following examples:

To find this string	Specify this term
the “Cancel” button	“the " “Cancel” " button”
computer “kltest16”	“computer " “kltest16”

This requirement does not apply to apostrophes, which are frequently used as quotes. Single quotes of this kind do not need escaping and should be specified in a plain string, as in **“local ‘Administrator’ user”.**

Filter Syntax

Select one of the operators (explained in the following table) and enter your filter terms.

Operator	Syntax	Example	Meaning
Contains	[FieldName]:	Name:Paul	The attribute contains all of the specified terms at once in any combination
Does not contain	NOT [FieldName]:	NOT Name:John	The attribute contains none of the specified terms anywhere
Equals	[FieldName]:	Name:“John Paul”	The attribute contents are identical to the specified phrase; do not enclose the phrase in quotation marks for this operator
Does not equal	NOT [FieldName]:	NOT SamAccountName:paul	The attribute contents are not identical to the specified phrase;

Do not enclose the phrase in quotation marks for this operator.

The following search syntax rules described above also apply to filter terms:

- Terms are case-insensitive
- The term can be a single word, multiple words, or a phrase in quotation marks.
- In single-word terms, a trailing asterisk is treated as a wildcard character
- In exact phrases, an asterisk is treated as a regular character.

Making Multi-Stage Searches

You have the option to run a search on the results of another search. It is a way to automate your established search practices, and it may provide a clearer and more convenient representation of your intentions.

This is similar to how the output of a command is redirected into another command as its input in PowerShell and Unix shell languages. Accordingly, search result redirection is provided by the familiar pipe (|) operator.

To indicate a field whose value should be carried over from the left query to the right through the pipe, enclose the field name in curly braces, as in {Where} or {EventID}. Example

```
"rd.itsearch" | What:Logon AND Who:"{SAMAccountName}" |
Name="{Where}"
```

In this three-stage search, the initial results are refined twice. First, it finds all users that are members of the **rd.itsearch** group. For these users, it finds such events that the users SAM account names are in the **Who** field, and the **What** field contains **Logon**. From the resulting events, pick only those that have any of the discovered computer names in the **Where** field.

Dashboards Module

CYBERQUEST Dashboards

A CYBERQUEST dashboard is a graphical representation of events (either circular or histograms) which can be accessed from **Dashboards** module interface when first logging in to application or by pressing



button at any time in left side, where is the quick access section of Web Interface.

Working with Dashboards module

After logging into the application, the Web Interface directs users to the Dashboards module, which offers a visual, real-time representation of all data contained in the online repository. This data is correlated and graphically presented to provide meaningful context regarding the organization's overall compliance.

The module operation area is divided in two sections:

- **Search and Filter** section allows you to granularly control what information is displayed in dashboards
- **Dashboards** section contains the dashgroups configured for the logged-in user

Search and Filter section

This section provides control over the information displayed in dashboards and allows defining additional filters and combination methods for searched data within a specified date and time interval. To access the Search and Filter section, expand Filters by pressing the

button, and will open:

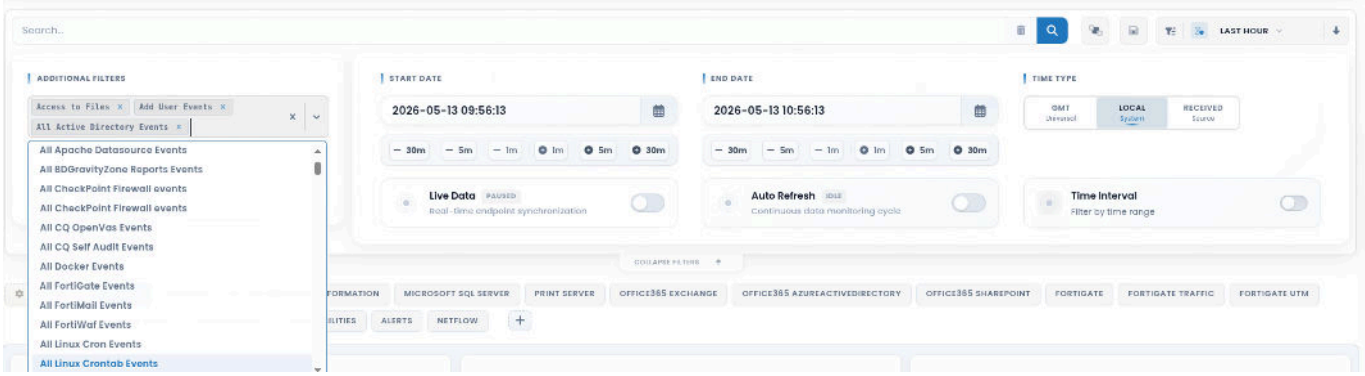


1)The Search field provides filtering of displayed information using free text input. If the field is left empty, all events are shown. A similar search field is available in the Browser module. A complete guide to using free text search capabilities is provided in this manual: Using Searches

- The Search Field also includes an autocomplete feature for default fields found in events, for example:



2. Additional filters can be specified using **Filtering options**. By default, no filters are selected. Accessing the **Additional filters** drop-down list presents a large collection of predefined filters sorted by technology, allowing selection of one or multiple filters. In **Filtering options**, the logical method for combining selected filters must be chosen from the **Combining method** drop-down list. Available options include the AND and OR logical operators. Note that the chosen operator applies to all selected filters.

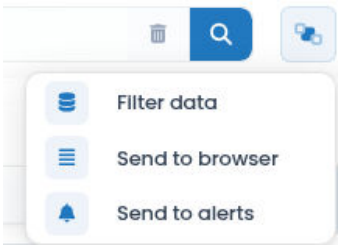


When finished, press



button to apply the selections.

Other options available in **Search and Filter** section:

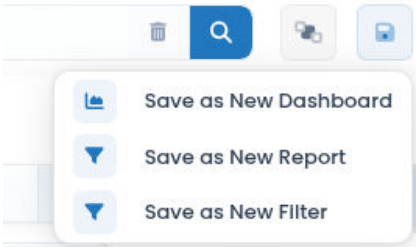


- The **Send to Browser** option directs the selection to the **Browser** module. This option opens a new web browser tab displaying the **Browser** interface with the filtered results.
- The **Send to Alerts** option directs the selection to the **Alerts** module. This option opens a new web browser tab displaying the **Alerts** interface with the filtered results.

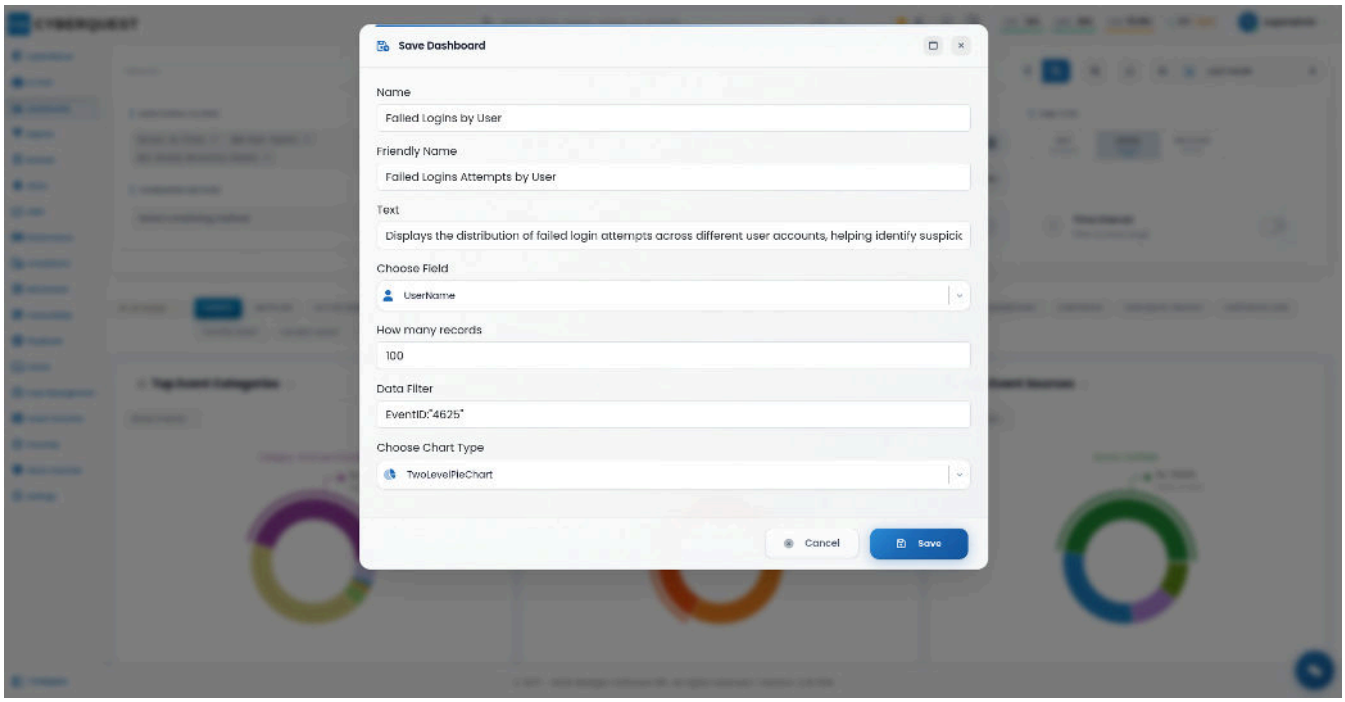
The current filter selection can be saved at any time. Pressing the



button presents three options for making the filter selection permanent:



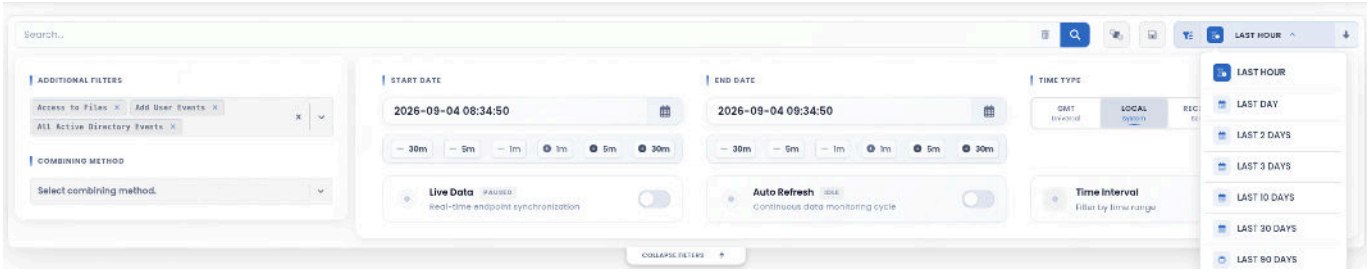
- The **Save as New Dashboard** option opens the **Save as New Dashboard** window, enabling the creation of a new dashboard. The following details must be specified:
  - A convention-based name for the dashboard, which will appear in dashboard lists
  - A descriptive, user-friendly name, displayed in the Dashboards interface
  - A description outlining the type of information presented in the dashboard
  - The field used for graph generation
  - How many records to display in the chart
  - A Data Filter that defines the search conditions to be applied for generating the dashboard content
  - Graphic type (barchart, pie, gauge etc.)



- The **Save as New Report** option opens the Save as New Report window, allowing the creation of a new report. A report name and description must be provided before the configuration can be saved.
- The **Save as New Filter** option opens the *Save as New Filter* window, enabling the creation of a new filter. A filter name and description must be specified before saving the configuration.

3)The **Search and Filter** section includes options for **setting the date and time interval** to define the time range of the displayed information. This feature provides a quick overview of compliance data over a specified period.

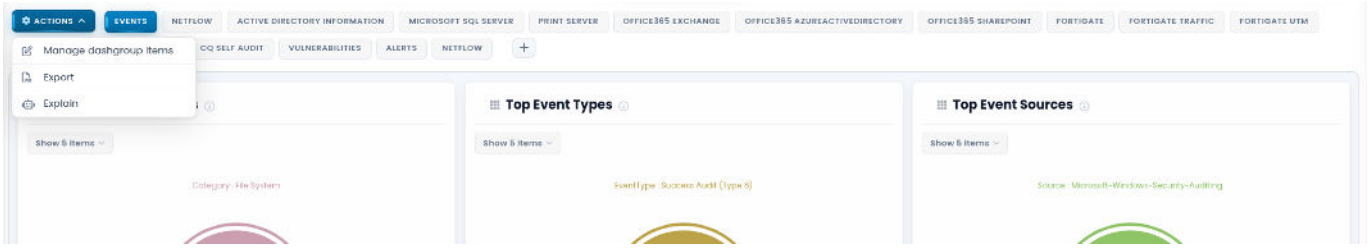
The interface provides options to define a specific start and end date, along with predefined date ranges (e.g., last hour, last day, last two days, last three days, last ten days, last 30 days, last 90 days). By default, the Dashboards interface displays data from the last hour. Additional controls beneath the **Start Date** and **End Date** fields allow for quick adjustment of the time interval and selection of the time reference to be used, including GMT, Local Time, ReceivedTime, Now, AutoRefresh, TimeInterval, and Not in this time interval.



- **GMT** - is the time reference which converts your search time into GMT (Greenwich Mean Time Zone).
- **LocalTime** - is the time reference when an event occurred.
- **ReceivedTime** - is the time reference when the events arrived in CYBERQUEST machine.
- **Now** - self-update end data with current time.
- **AutoRefresh** - refreshes the page every 10 seconds.
- **Time Interval** - the search is made from Start Time to End Time interval
- **Not in this time interval** - the search outputs the events that are NOT between Start Time and End Time

Dashboards section

This is the main display area for user dashboards. A logged in user will be presented with actionable dashgroups that are set for his profile. By clicking on a dashgroup, the user will be able to display dashboards that are included in that dashgroup.



Possible actions are:

- **Select - **Clicking on a dashgroup displays the dashboards included in that group. For the selected dashgroup, there is the option to quickly add or edit dashboards within it.
- **Add dashgroup –** Pressing the

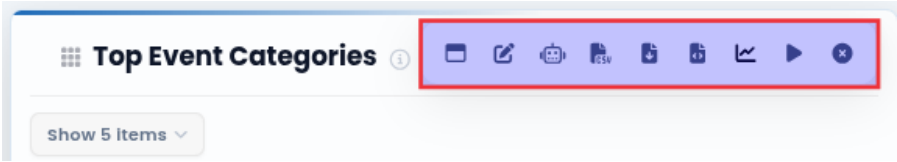
  button at the end of the dashgroups row allows quick creation of a new dashgroup under the current profile. Dashboards can then be added to a dashboard group by opening the **Actions** menu and selecting **Manage Dashgroup Items**.
- **Export dashgroup** - Enables the export of events from Dashgroups based on a specified time period and filtered through the Search Field.

  For detailed instructions on exporting data from a Dashgroup, refer to the following link: [How to export data from dashgroup](#).

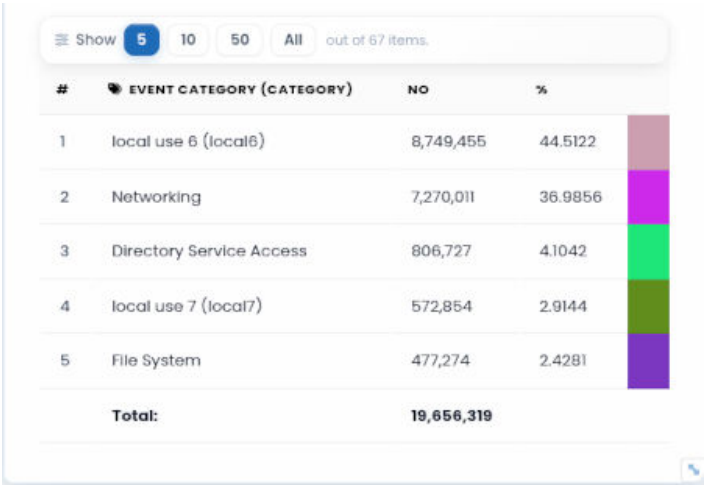
- **Delete dashgroup -** Each dashgroup selector includes a remove button in the top-right corner, visible on mouse hover. Selecting this button permanently deletes the dashgroup. Dashboards linked to the deleted dashgroup are not removed and can be reassigned to another dashgroup as needed.

When a dashgroup is selected, its associated dashboards are displayed in the Dashboards interface. For each listed dashboard, available actions become visible on mouse hover:

- A set of quick-action buttons is available in the top-right corner of the dashboard:



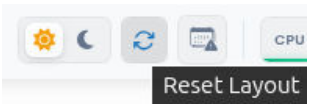
- **Maximize/Minimize -** Expands the dashboard to fill the entire display area or returns it to its original size.
- **Export to CSV -** Generates a CSV file containing the events displayed in the dashboard.
- **Export Dashboard Object -** Export the dashboard's definition in a proprietary format.
- **Graph selection -** Opens a drop-down list of available graphical formats for dashboards, enabling quick changes to the display format of the dashboard. These changes do not affect the dashboard definition and will revert upon the next load.
- **Explain** opens the AI Chat with a contextual interpretation of the selected dashboard, helping users understand what the displayed data means and why it may be relevant. The AI assistant summarizes the dashboard, highlights key patterns or anomalies, and provides analyst-friendly explanations to support faster investigation and decision-making.
- **Add to Slideshow** - Adds the selected dashboard to the slideshow list. Multiple relevant dashboards can be added and arranged in the desired display order. The slideshow can be configured with a display interval and started in presentation mode, automatically cycling through the selected dashboards.
- **Edit dashboard** - Enables editing and permanent modification of the dashboard definition:



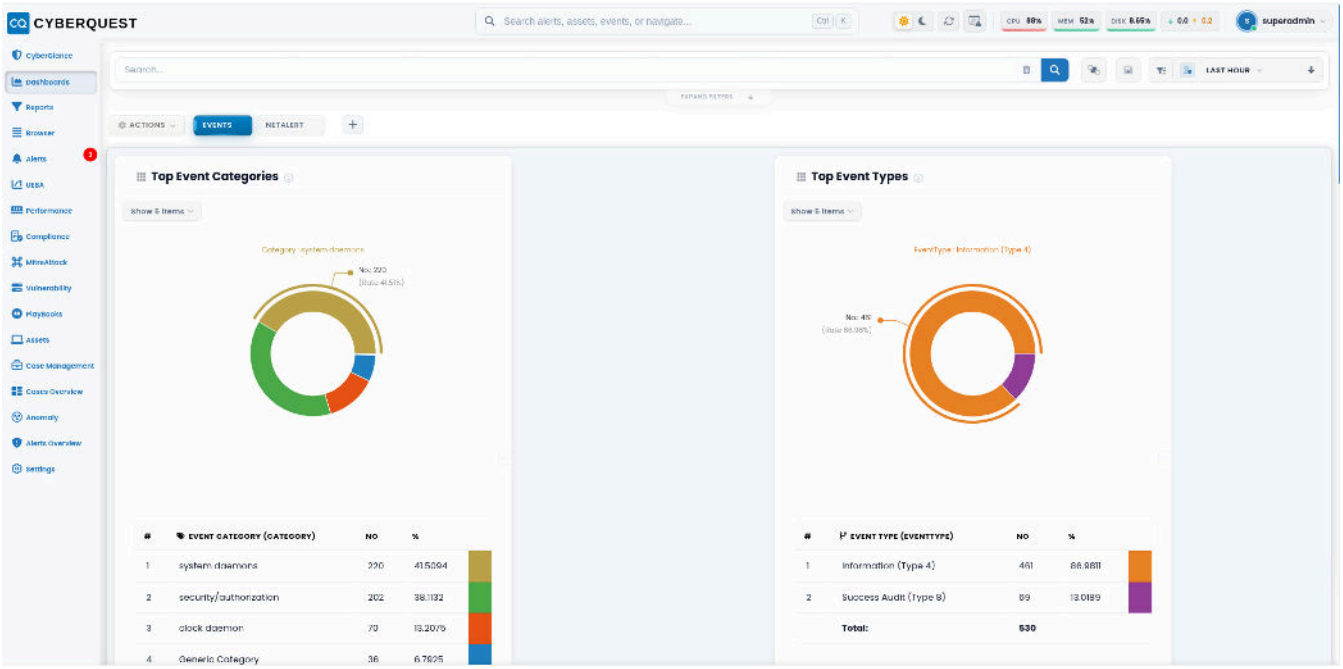
- Show option modifies the maximum number of entries displayed in the dashboard.

  Since the purpose of the Dashboard interface is to provide a real-time overview of the monitored environment, the number of events displayed is limited.

  Dashboards can be repositioned by pressing and holding while dragging the cursor. They can also be expanded or resized as needed. To restore the default layout, click the

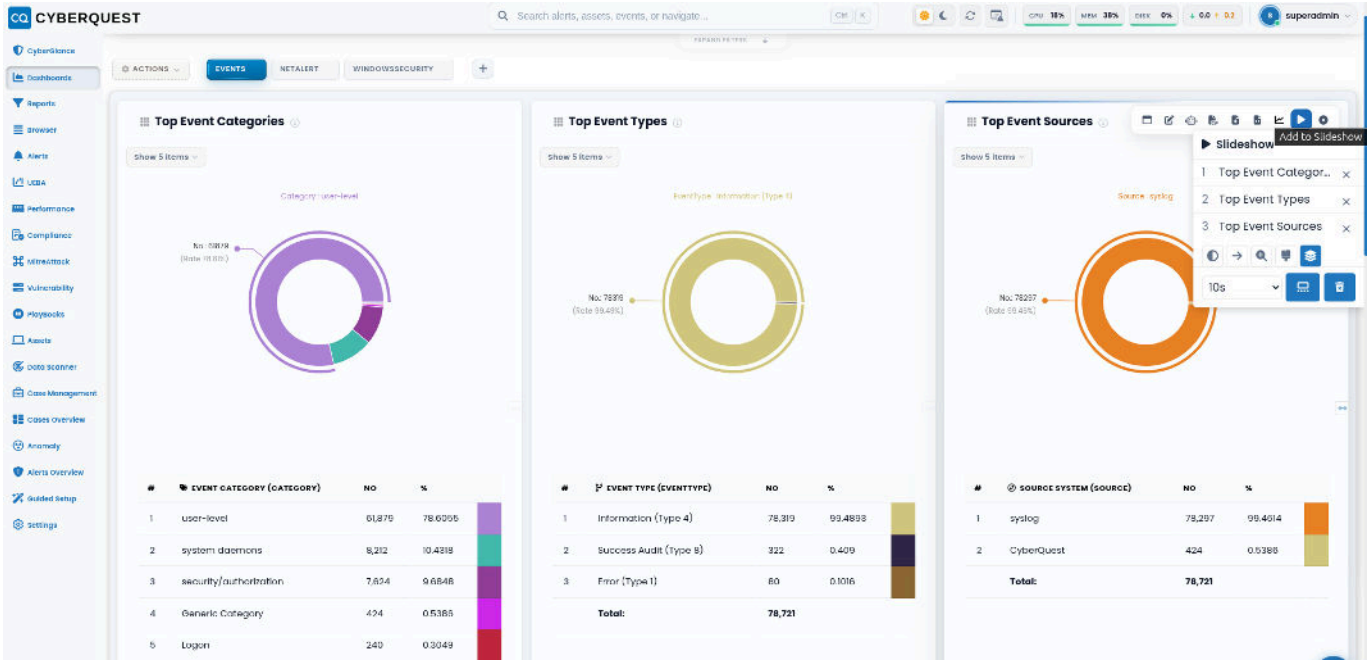


  button from the top-right corner of interface.

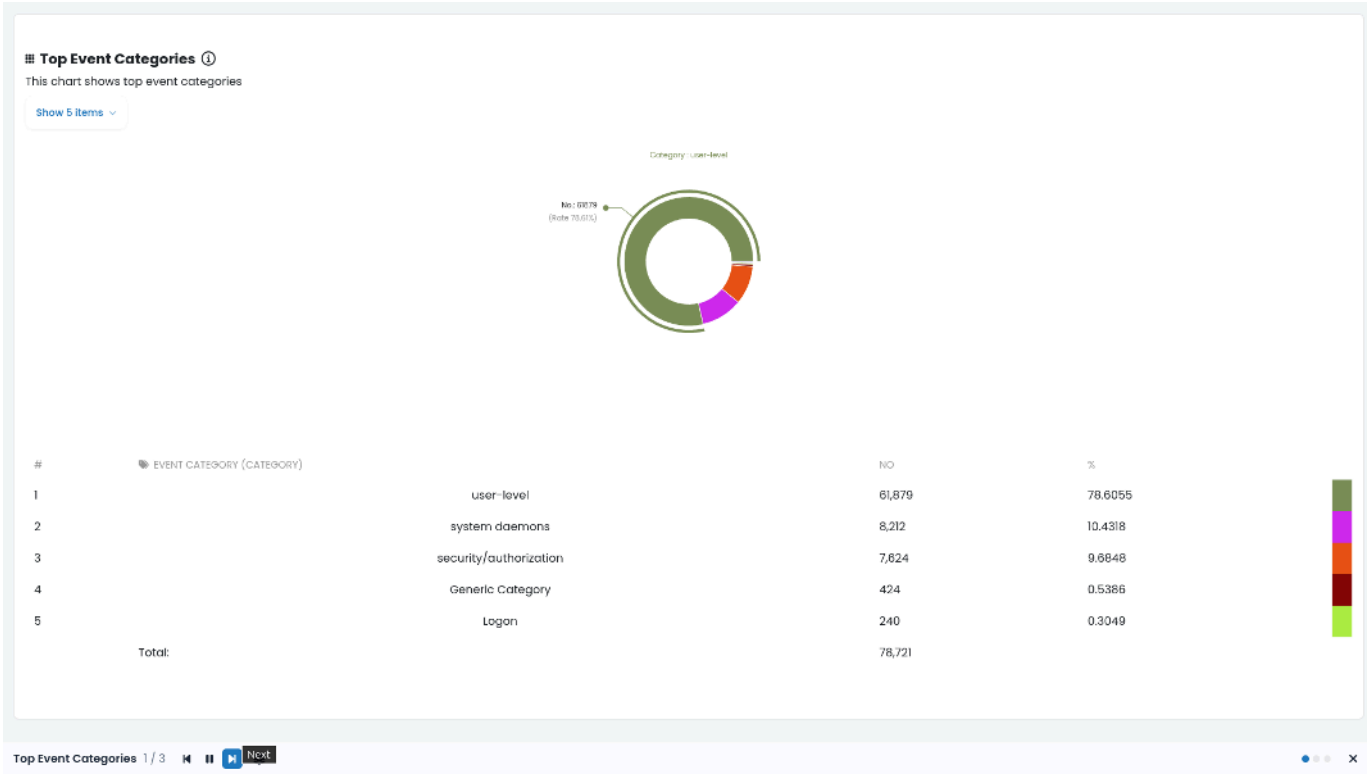


Dashboard Slideshow

CYBERQUEST allows users to create a slideshow from selected dashboards for continuous monitoring or presentation purposes. Dashboards can be added individually to the slideshow, arranged in the required order, and displayed automatically using a configurable time interval.



Once the slideshow is started, each selected dashboard is displayed sequentially and can be viewed in fullscreen mode.



Types of dashboards

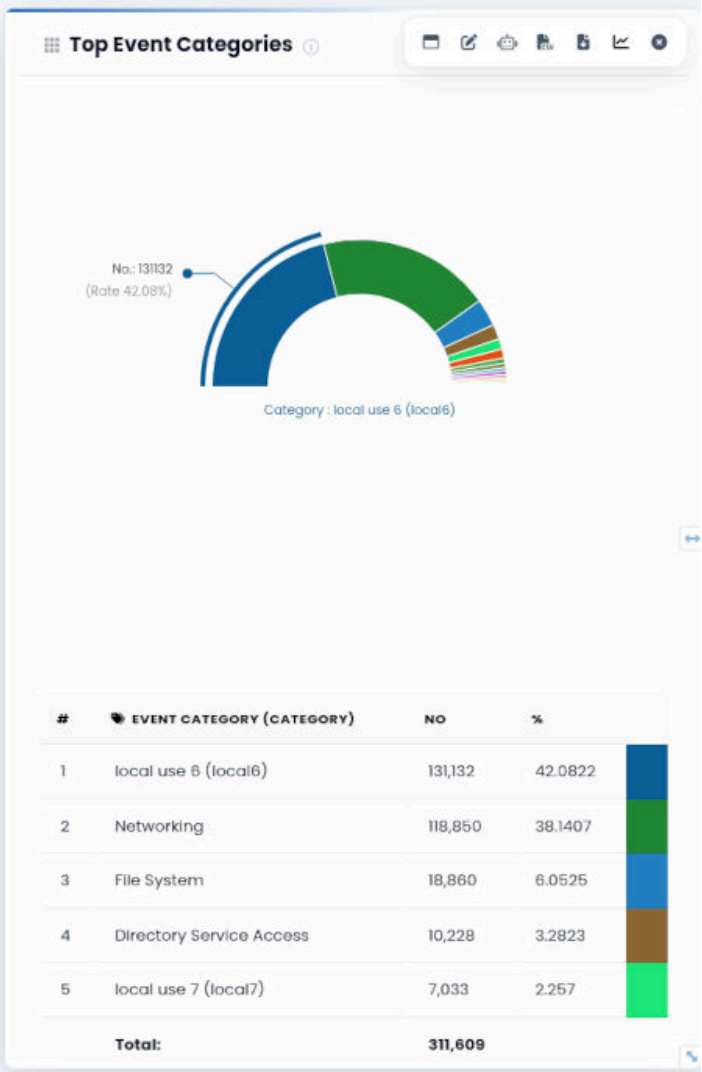
Dashboards are organized into different categories. The most representative are:

- Event related charts
- Network related charts
- Active Directory related charts
- ALERTS related charts

Event related charts

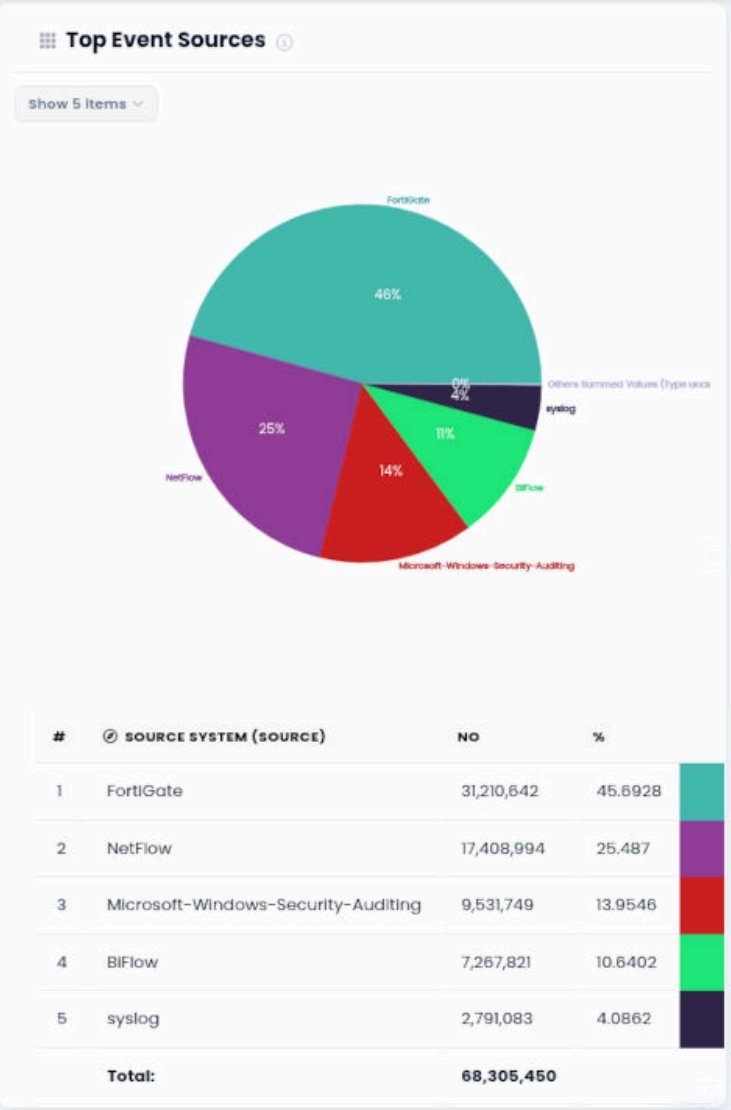
Represent the dashboards built on events collected from various sources. Below are the most commonly used:

- **Gauge** chart in reference to the top events categories



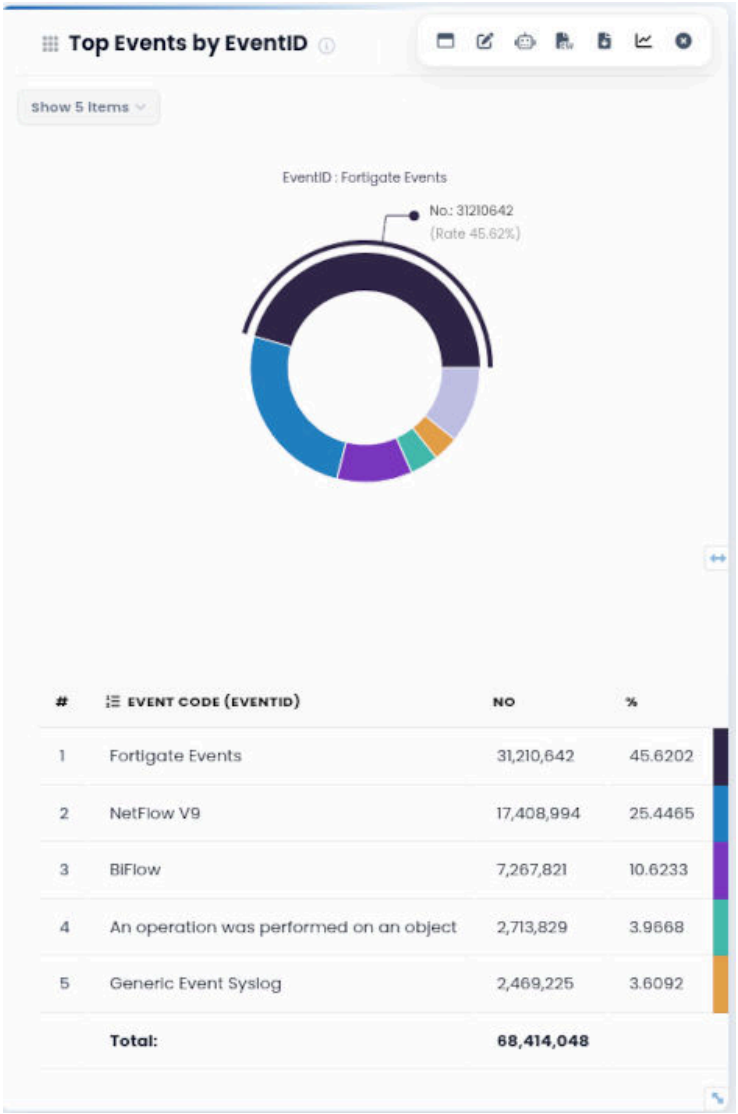
#	EVENT CATEGORY (CATEGORY)	NO	%
1	local use 6 (local6)	131,132	42.0822
2	Networking	118,850	38.1407
3	File System	18,860	6.0525
4	Directory Service Access	10,228	3.2823
5	local use 7 (local7)	7,033	2.257
	Total:	**311,609**	

- **Pie** chart in reference to event sources

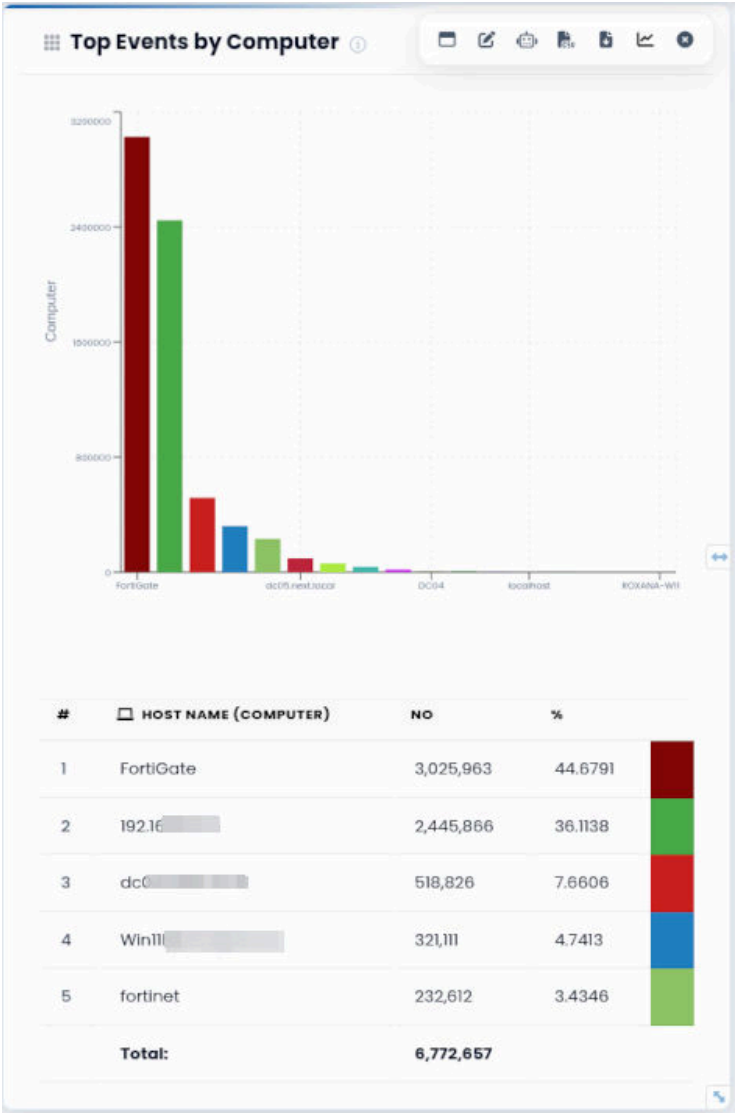


#	SOURCE SYSTEM (SOURCE)	NO	%
1	FortiGate	31,210,642	45.6928
2	NetFlow	17,408,994	25.487
3	Microsoft-Windows-Security-Auditing	9,531,749	13.9546
4	BiFlow	7,267,821	10.6402
5	syslog	2,791,083	4.0862
	Total:	**68,305,450**	

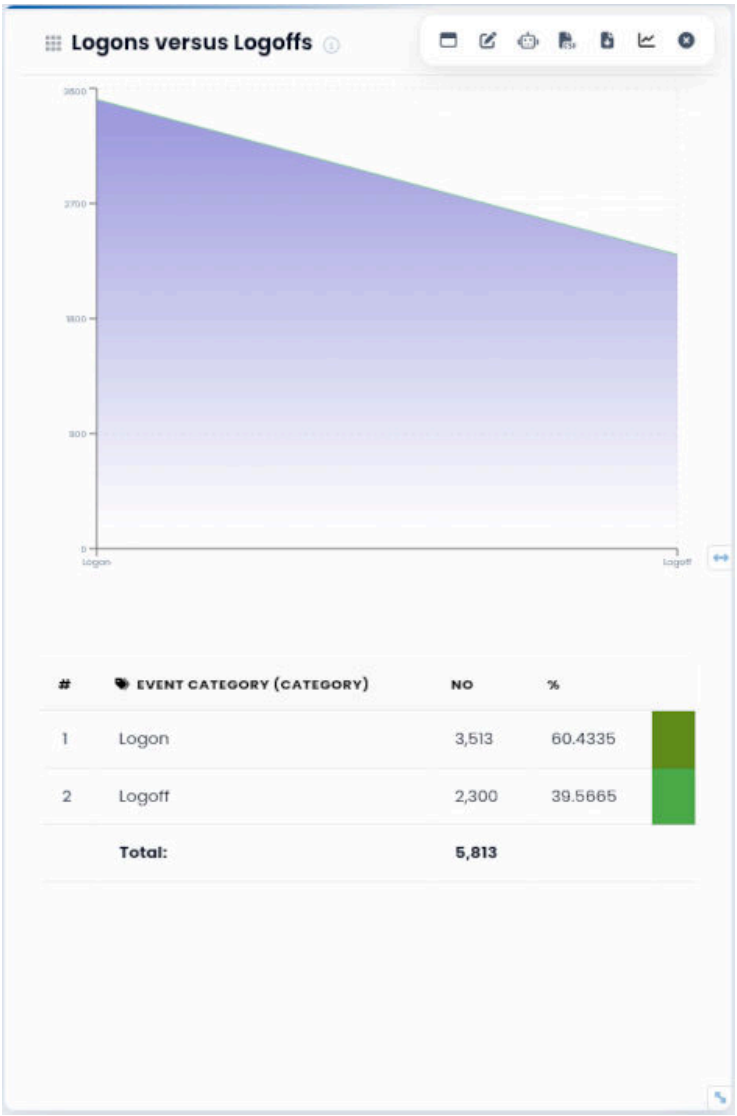
- **Two-Level Pie** chart in reference to event ID



- The **Barchart** in reference to the computer that generated the event



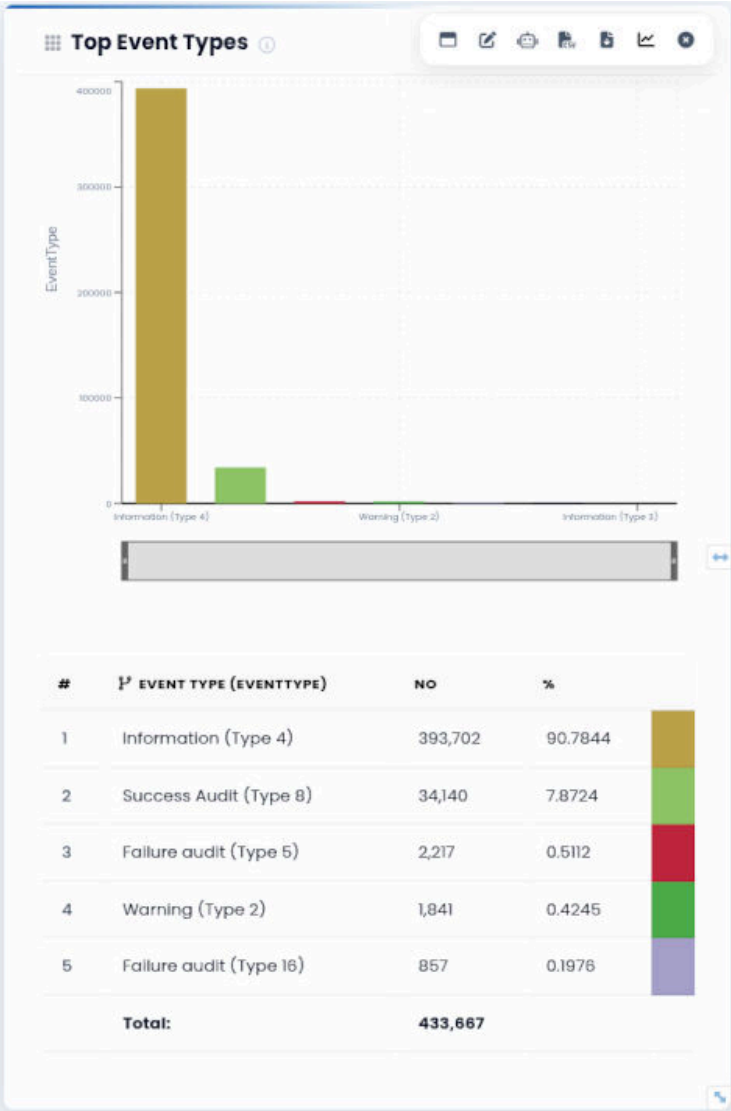
- **AreaChart** in reference to the proportion between logons and logoffs



- **LineChart** about the distribution of events over a selected time interval

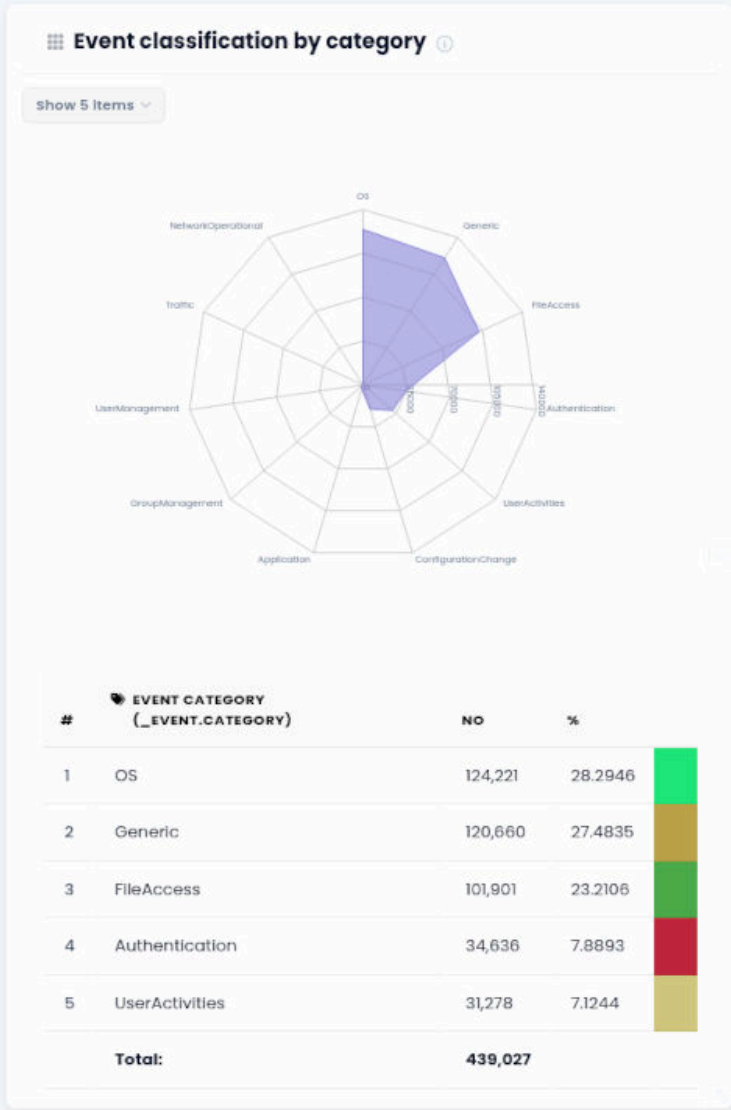


- **BrushBarChart** - chart reference to top events types



#	EVENT TYPE (EVENTTYPE)	NO	%
1	Information (Type 4)	393,702	90.7844
2	Success Audit (Type 8)	34,140	7.8724
3	Failure audit (Type 5)	2,217	0.5112
4	Warning (Type 2)	1,841	0.4245
5	Failure audit (Type 16)	857	0.1976
	Total:	**433,667**	

- **RadarChart** the chart shows the classification event by category



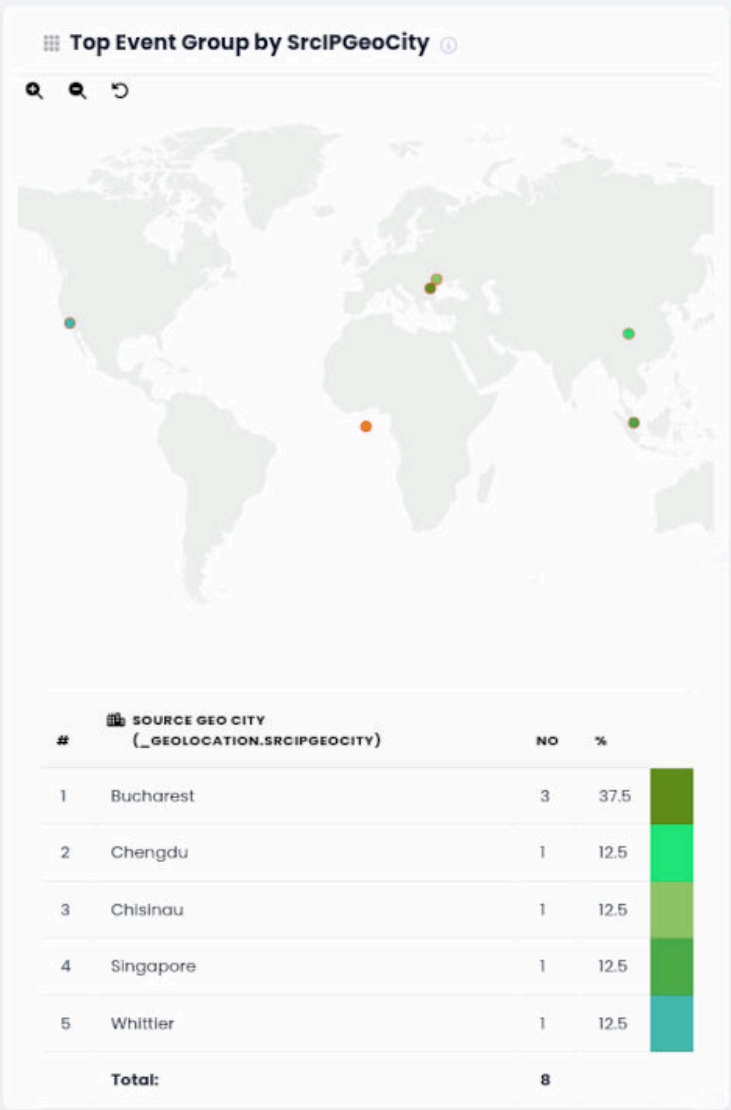
#	EVENT CATEGORY (_EVENT.CATEGORY)	NO	%
1	OS	124,221	28.2946
2	Generic	120,660	27.4835
3	FileAccess	101,901	23.2106
4	Authentication	34,636	7.8893
5	UserActivities	31,278	7.1244
	Total:	**439,027**	

- **WorldMap** the chart shows the events group by SrcIPGeoCountry



#	SOURCE GEO COUNTRY (_GEOLOCATION.SRCIPGEOCOUNTRY)	NO	%
1	Romania	3	23.0769
2	Bulgaria	2	15.3846
3	United States	2	15.3846
4	Australia	1	7.6923
5	China	1	7.6923
	Total:	**13**	

- **WorldMapCities** the chart shows events by SrcIPGeocity



#	SOURCE GEO CITY (_GEOLOCATION.SRCIPGEOCITY)	NO	%
1	Bucharest	3	37.5
2	Chengdu	1	12.5
3	Chisinau	1	12.5
4	Singapore	1	12.5
5	Whittier	1	12.5
	Total:	**8**	

- **Spline Chart** shows the Top Event Types and visualizes their distribution by event count.

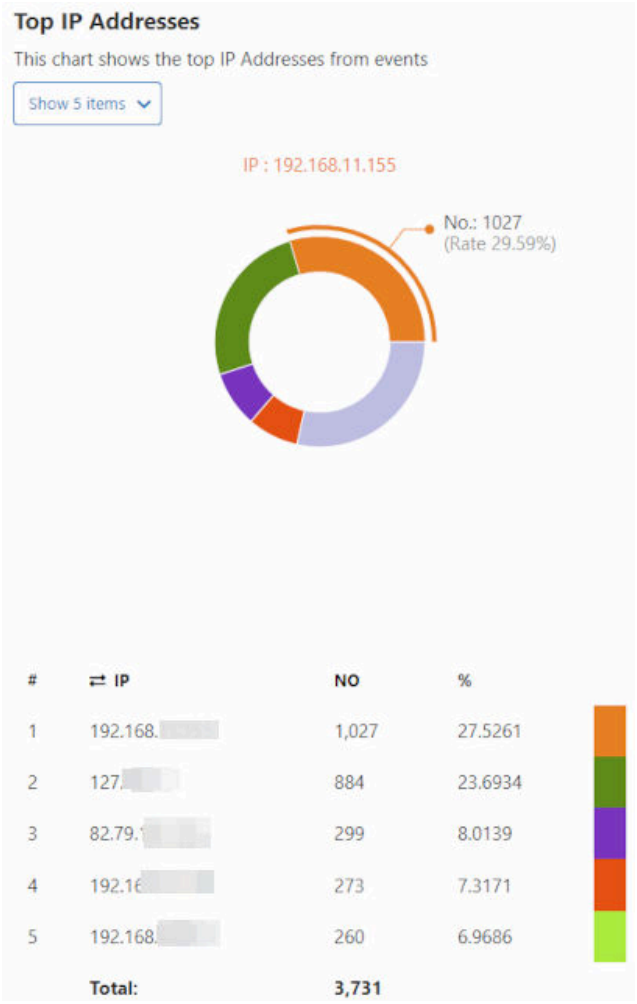


#	EVENT TYPE (EVENTTYPE)	NO	%
1	Success Audit (Type 8)	5,272,043	37.4541
2	Information (Type 4)	5,164,434	36.6896
3	Information (Type 0)	1,810,837	12.8647
4	Warning (Type 2)	1,810,376	12.8614
5	Error (Type 1)	17,092	0.1214

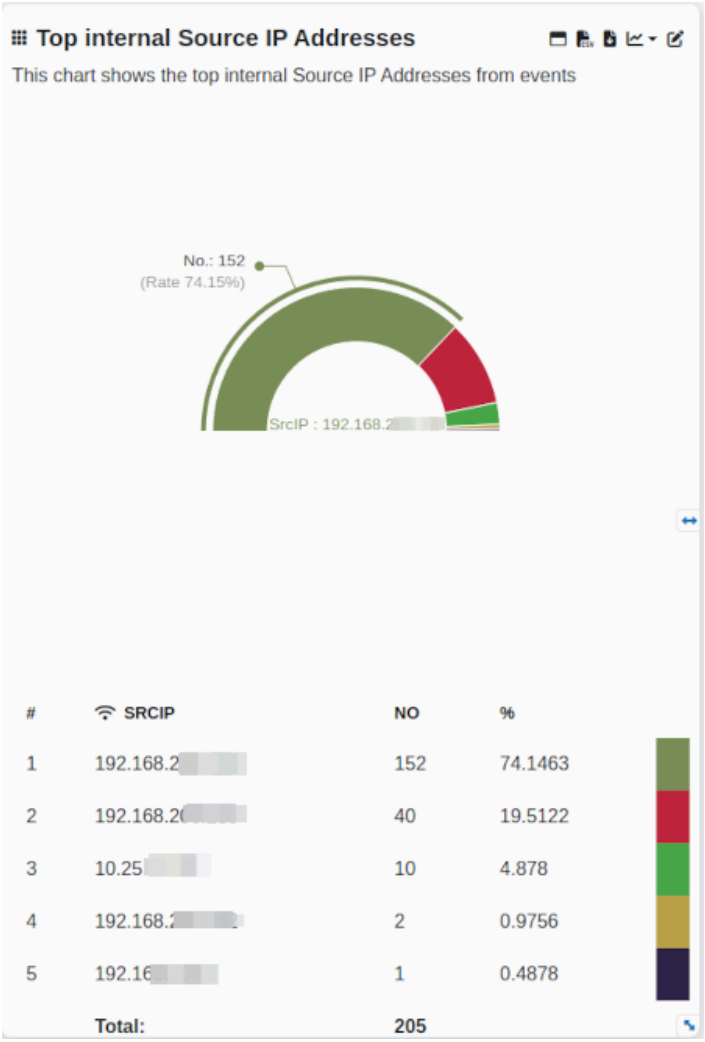
Network related charts

Represent the dashboards built on flow collected from NetFlow or other type of network flow sources. Below are the most commonly used:

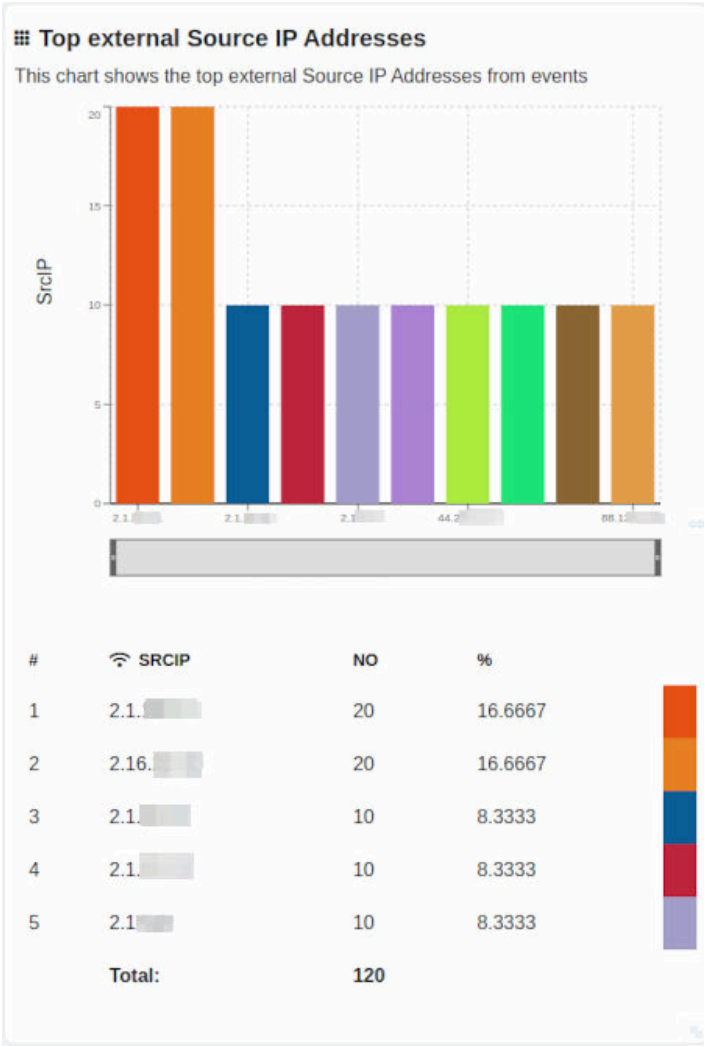
- **Two-Level Pie** chart in reference to Top IP addresses found in logs



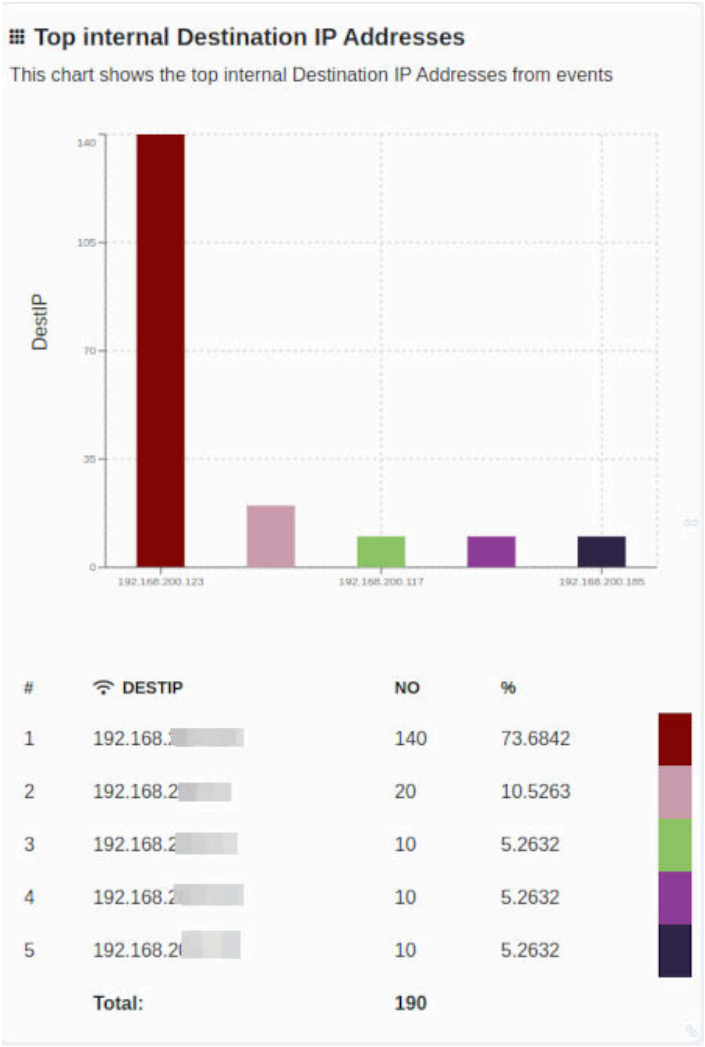
- **Gauge** chart in reference to internal IP addresses identified in events



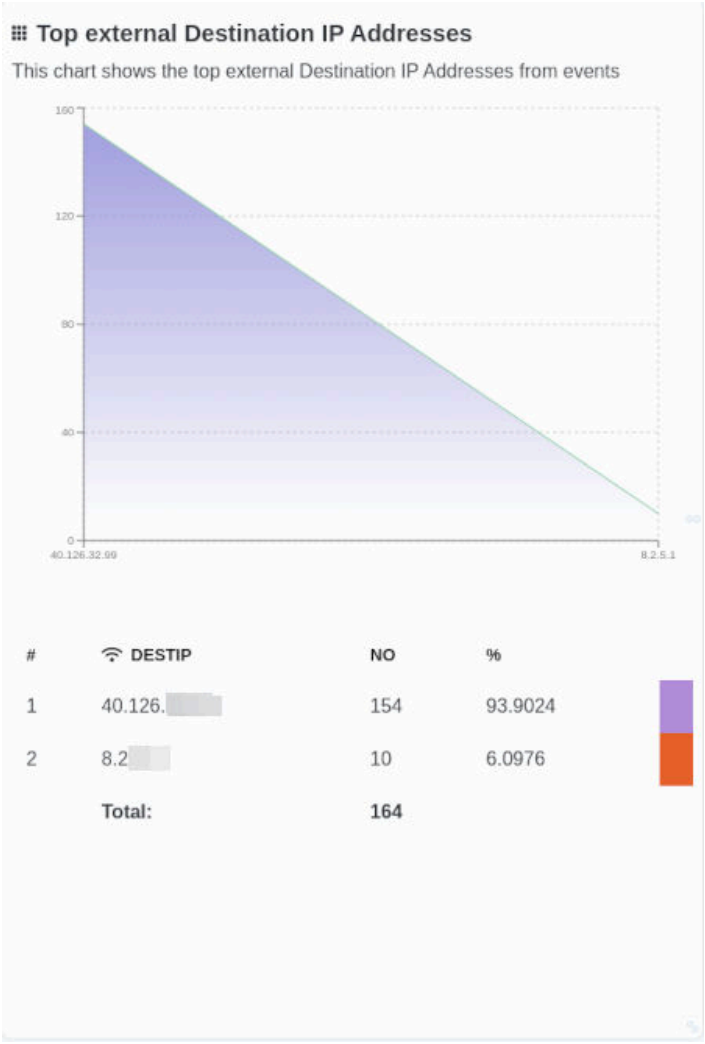
- **BarChart** in reference to external IP addresses identified in events



- **BrushBarChart** the chart shows the Top Internal Destination IP Addresses from events



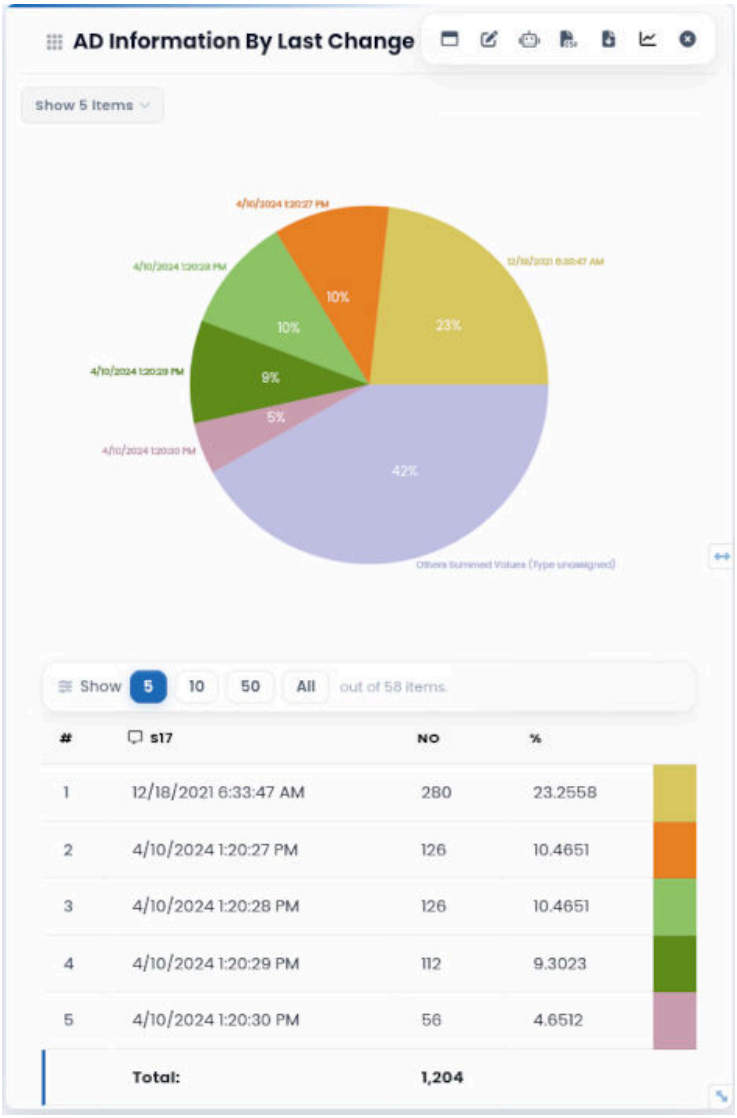
- **AreaChart** the chart shows the Top extDestination IP Addresses from events



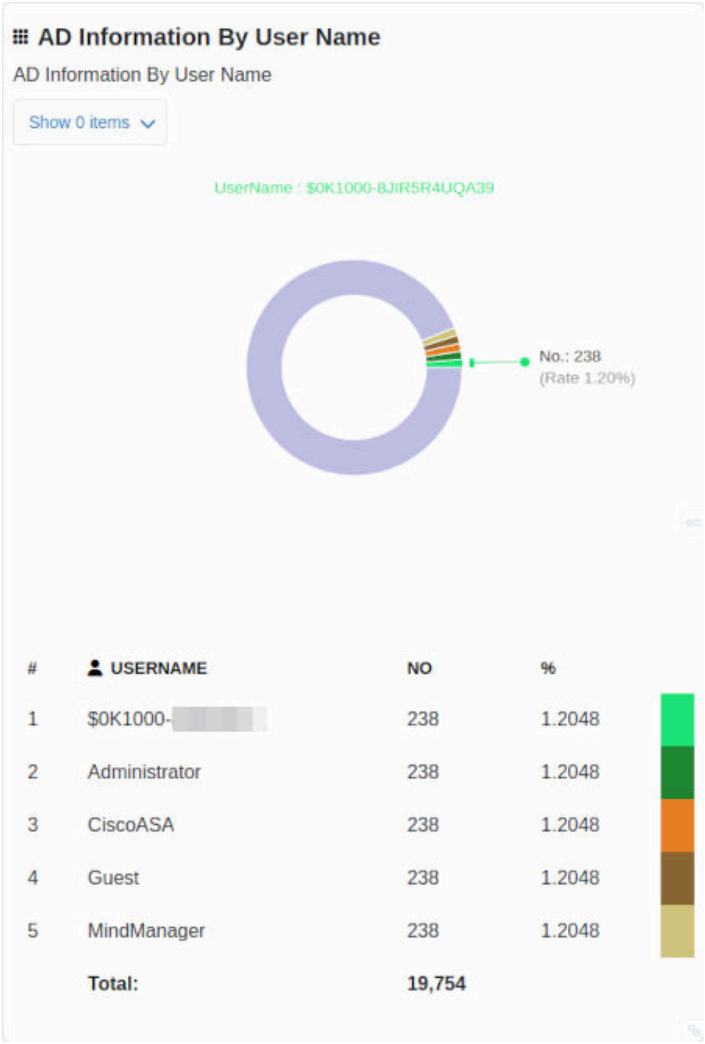
Active Directory (or other) related charts

Represent the dashboards built on additional information collected from Windows Active Directory and other sources of information using a correlation between events and WMI, SNMP or other type of network flow sources. Below are the most commonly used:

- **Pie** in reference to Last Change - Active Directory Events by Last Change



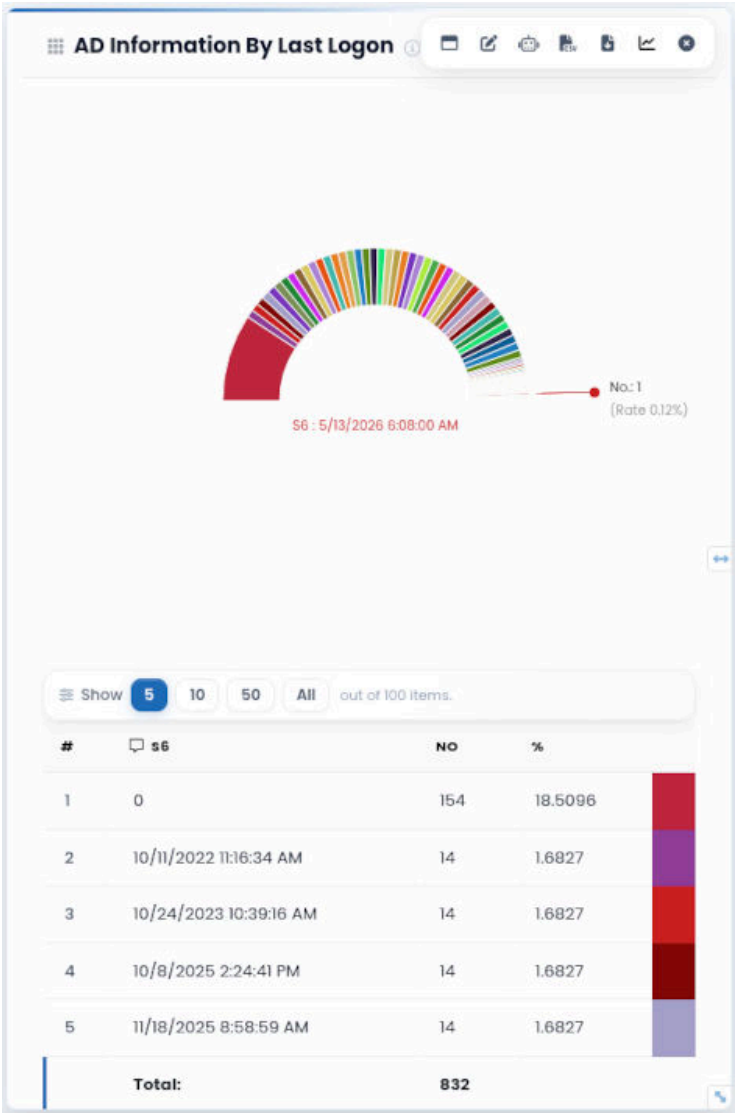
- **Two-Level Pie** chart in reference to User Name



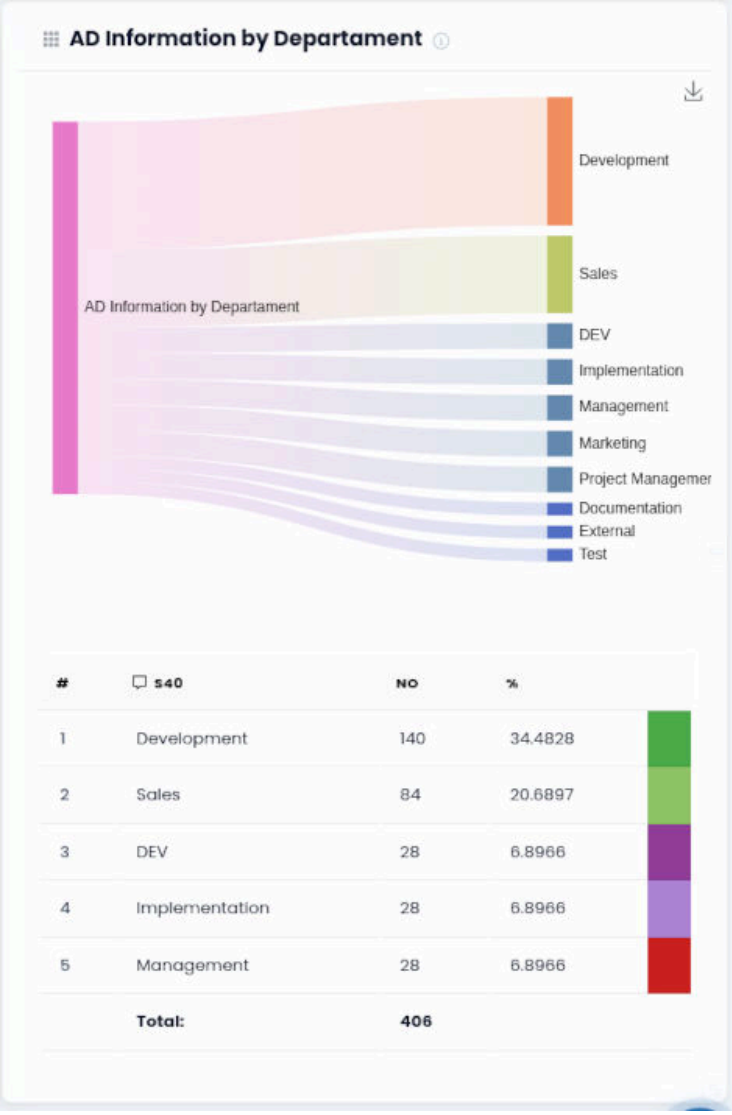
- **Line Chart** chart in reference to Pass Never Expire



- **Gauge** chart in reference to Active Directory events by Last Logon

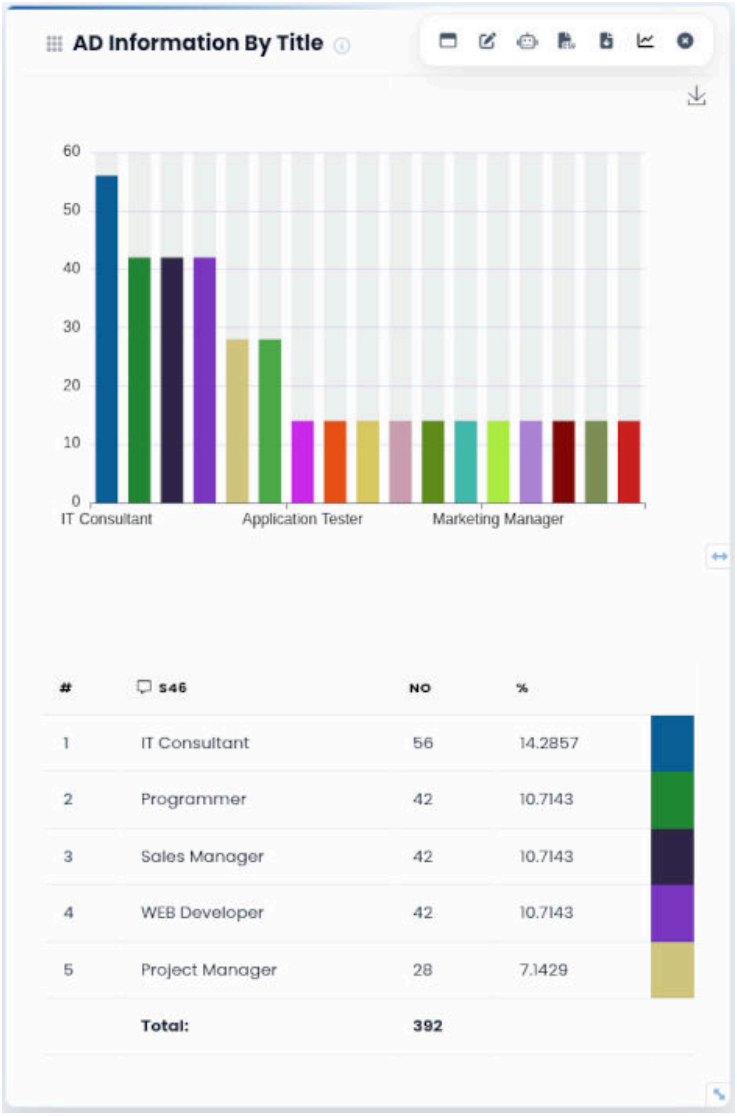


- **Echart Sankey Chart** shows the distribution of **Active Directory users by department**, making it easy to identify the largest AD user groups.



#	s40	NO	%
1	Development	140	34.4828
2	Sales	84	20.6897
3	DEV	28	6.8966
4	Implementation	28	6.8966
5	Management	28	6.8966
	Total:	**406**	

- **Echart Bar Chart** shows the distribution of AD records by job title, highlighting the most common roles and their percentage share.

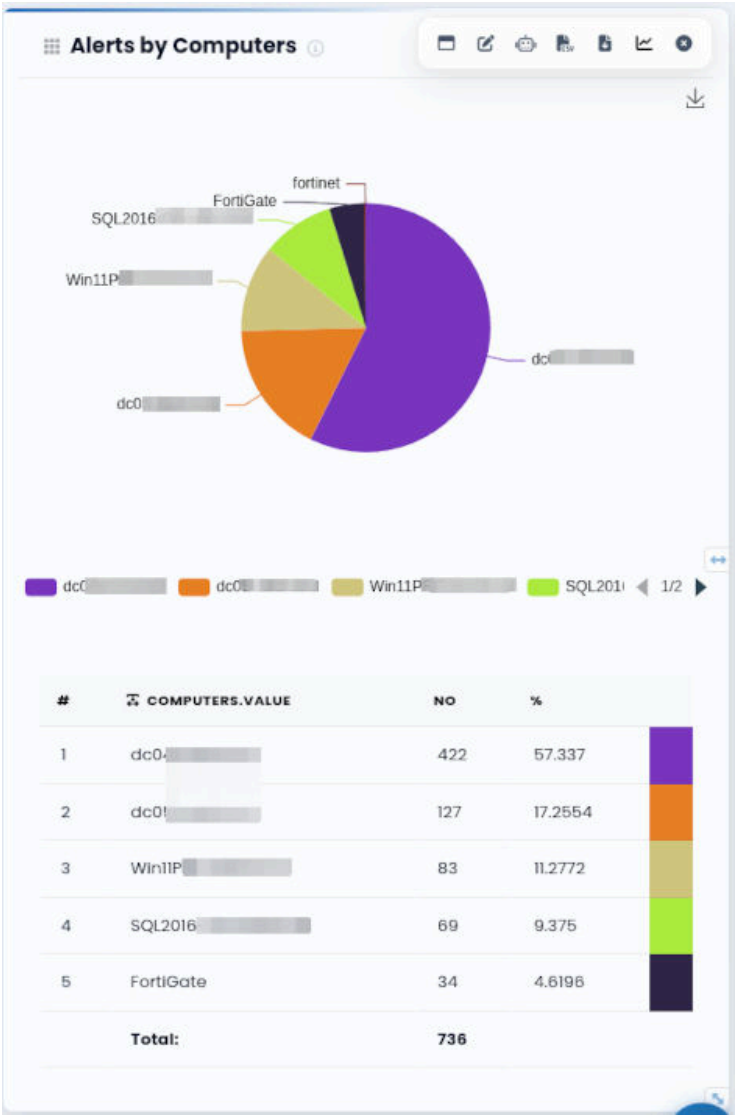


#	S46	NO	%
1	IT Consultant	56	14.2857
2	Programmer	42	10.7143
3	Sales Manager	42	10.7143
4	WEB Developer	42	10.7143
5	Project Manager	28	7.1429
	Total:	**392**	

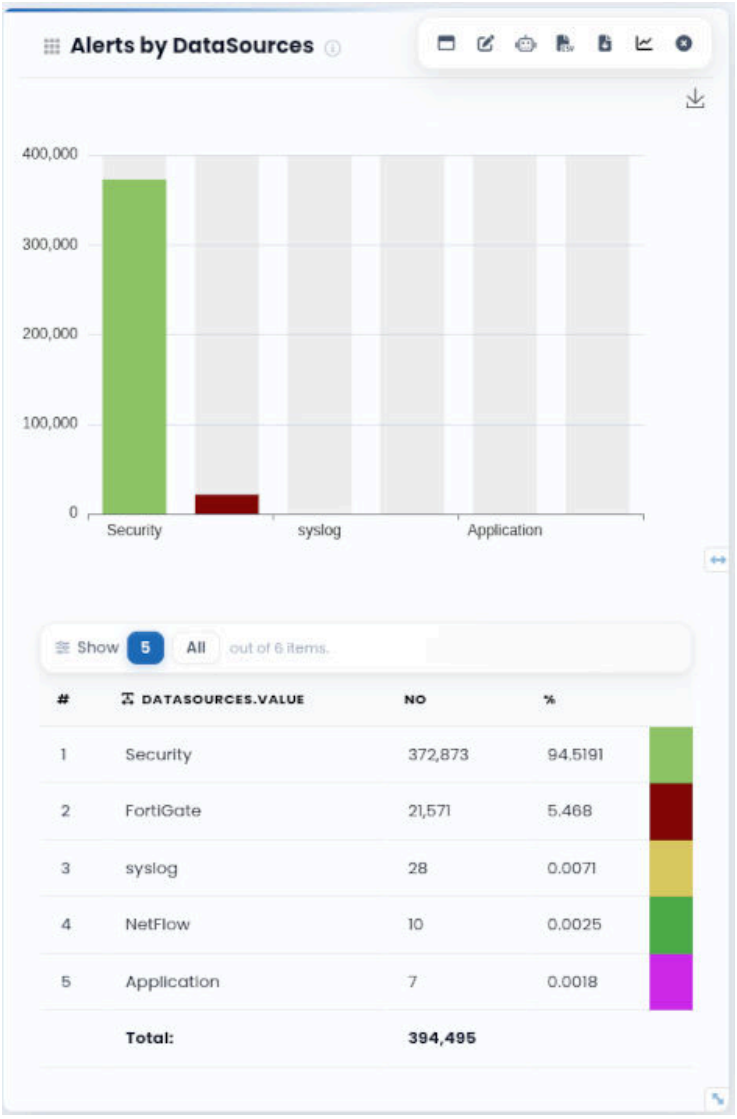
Alerts related charts

Represent the dashboards built on alerts collected from various sources. Below are the most commonly used:

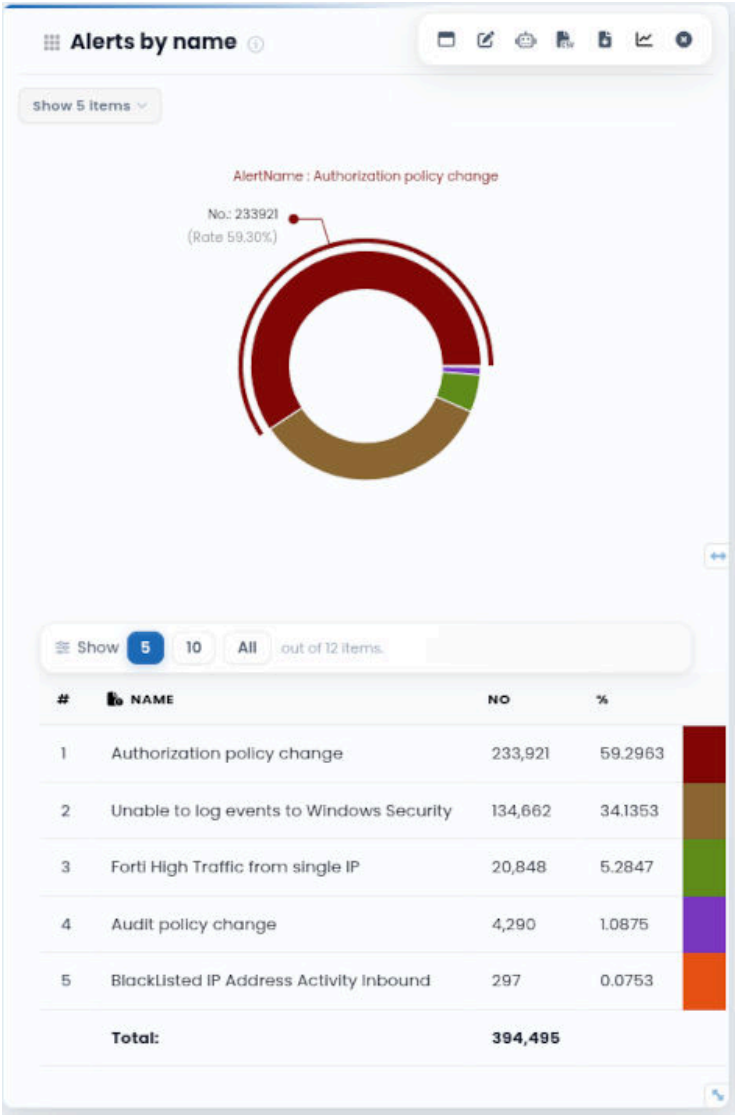
- **Echart Pie Chart** shows the Alerts by Computers



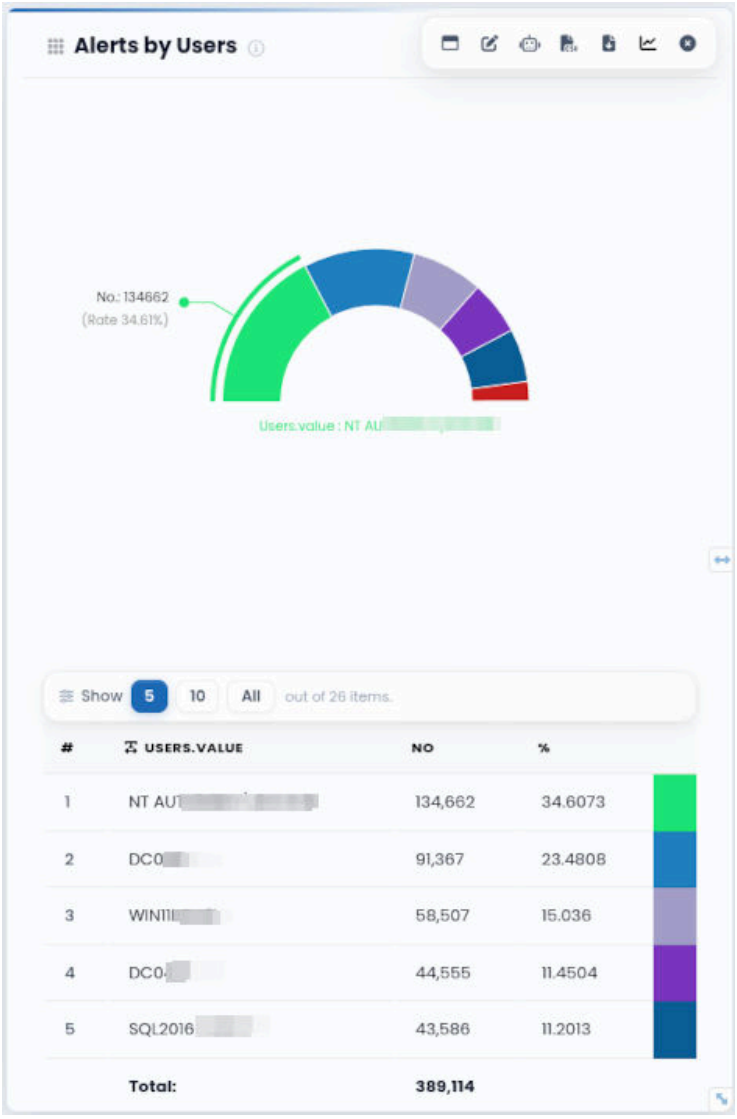
- **Echart Bar Chart** shows the Alerts by DataSources



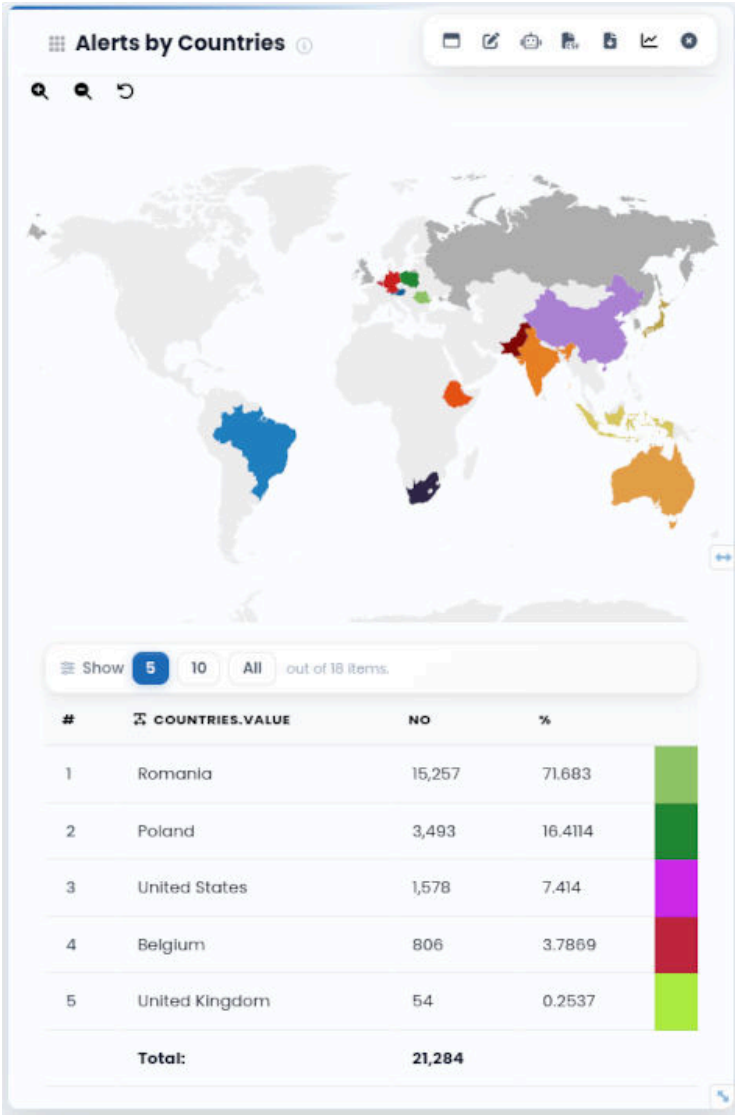
- **TwoLevelPie Chart** shows the Alerts by name



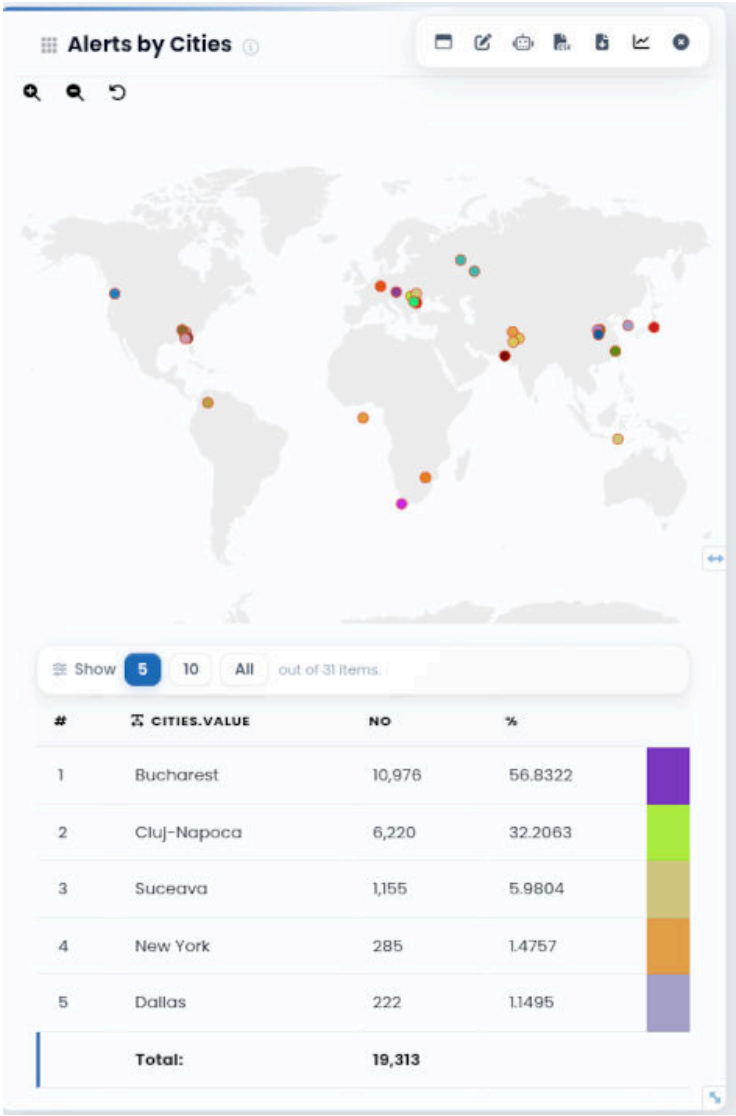
- **Gauge** shows the Alerts by Users



- **WorldMap** shows the Alerts by Countries



- **WorldMap Cities** shows the Alerts by Cities



How to create a new dashboard, dashgroup and view data

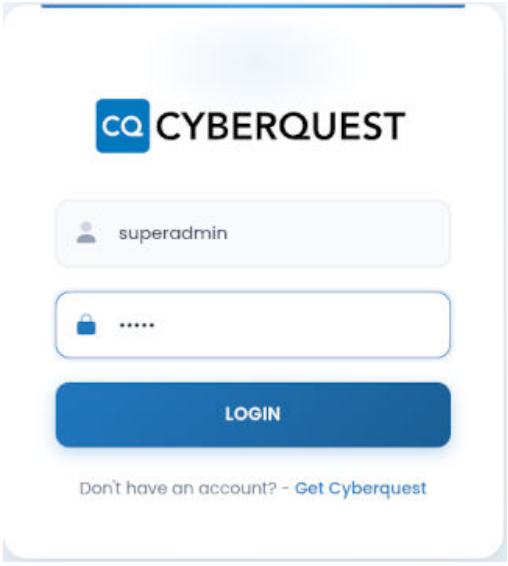
A CYBERQUEST dashboard is a graphical representation of events (displayed as circular charts or histograms) that can be accessed through the **Dashboards** module upon logging into the application, or at any time by clicking the "Dashboards" button in the top-left section of the Web Interface.

How to create a new dashboard

Authentication

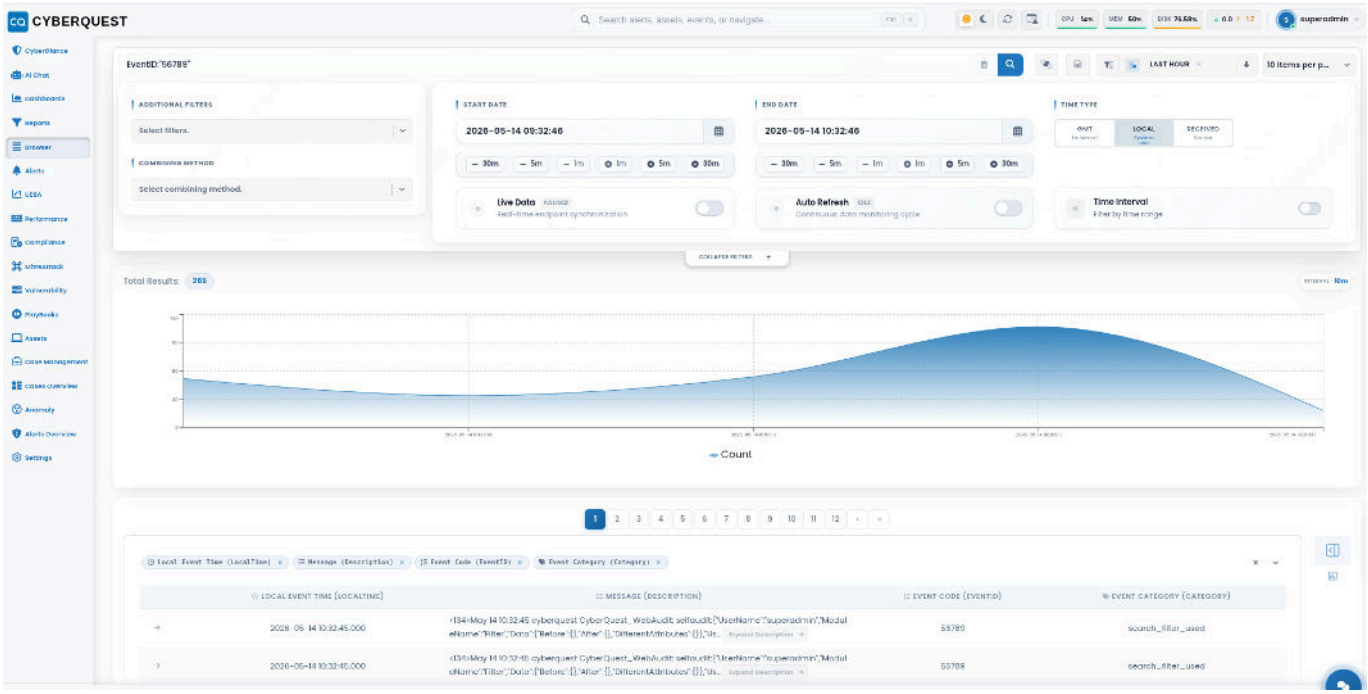
To access Web Interface, open a web browser and type the application's address or DNS name. The default address initially assigned to Web Interface is ***https://CyberquestIPAddress*** (example).

The browser automatically redirects you to CYBERQUEST's authentication page:



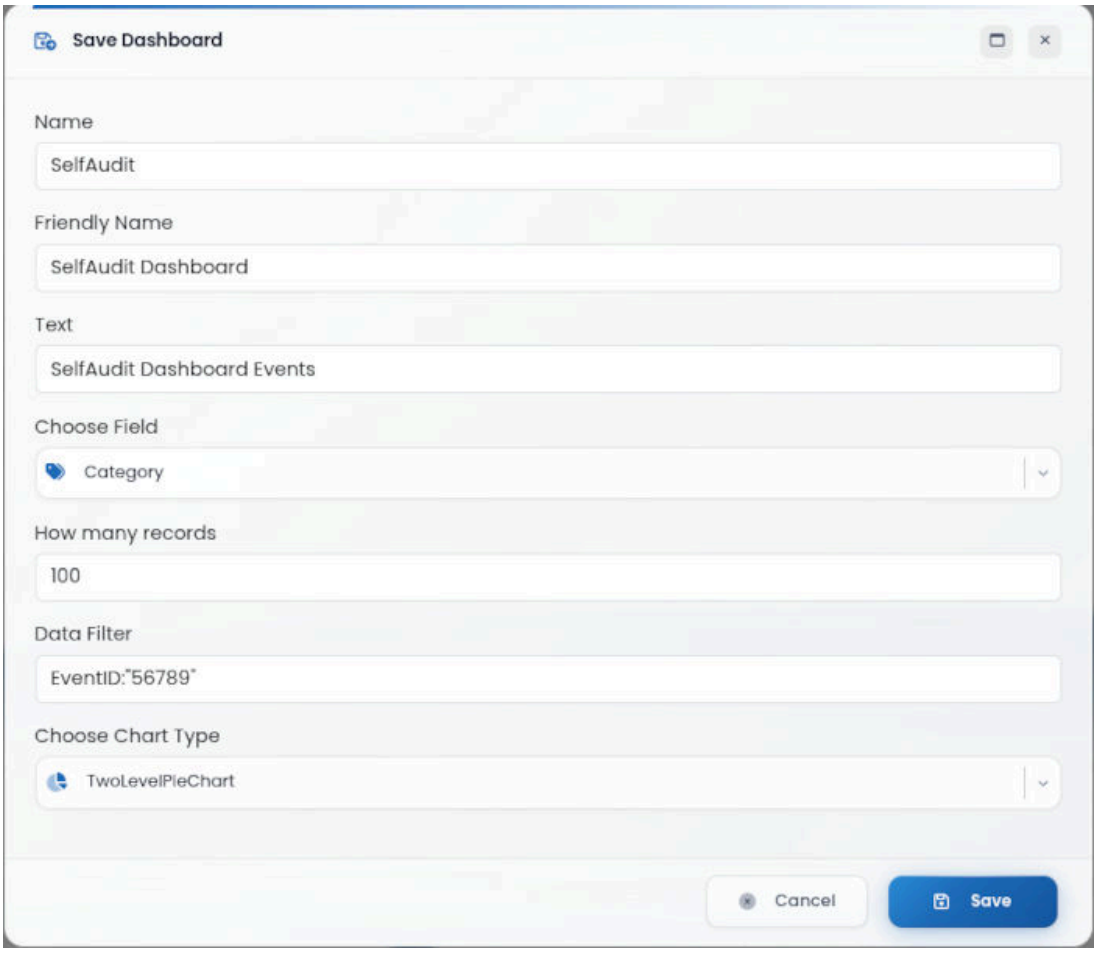
Navigate to browser page

Navigate to the "Browser" page. Create a filtering rule - for example, filter self-audit events using EventID:"56789". Then save the configuration as a dashboard by clicking **SAVE OPTIONS > Save as New Dashboard**.



Complete the form

Complete the form with the appropriate information and press the "Save" button:



Name: The name of the new Dashboard;

Friendly Name: A descriptive, user-friendly name for the new dashboard. This name will be displayed in the Dashboards interface.

Text: A descriptive text detailing the information presented in the new dashboard.

Choose Field: The field used to aggregate data within the dashboard.

How many records: The number of events to include.

Data Filter: The filter criteria used to generate the dashboard.

**Choose Chart Type: **The type of chart to represent the dashboard data.

How to create a new dashgroup

This is the main display area for user dashboards. Upon logging in, the user is presented with actionable dashgroups configured for their profile. By clicking on a dashgroup, the user can view the dashboards it contains.

Follow these steps to create a new dashgroup:

Add dashgroup

Navigate to the “Dashboards” page and click the “ADD DASHGROUP” button or the plus button



.

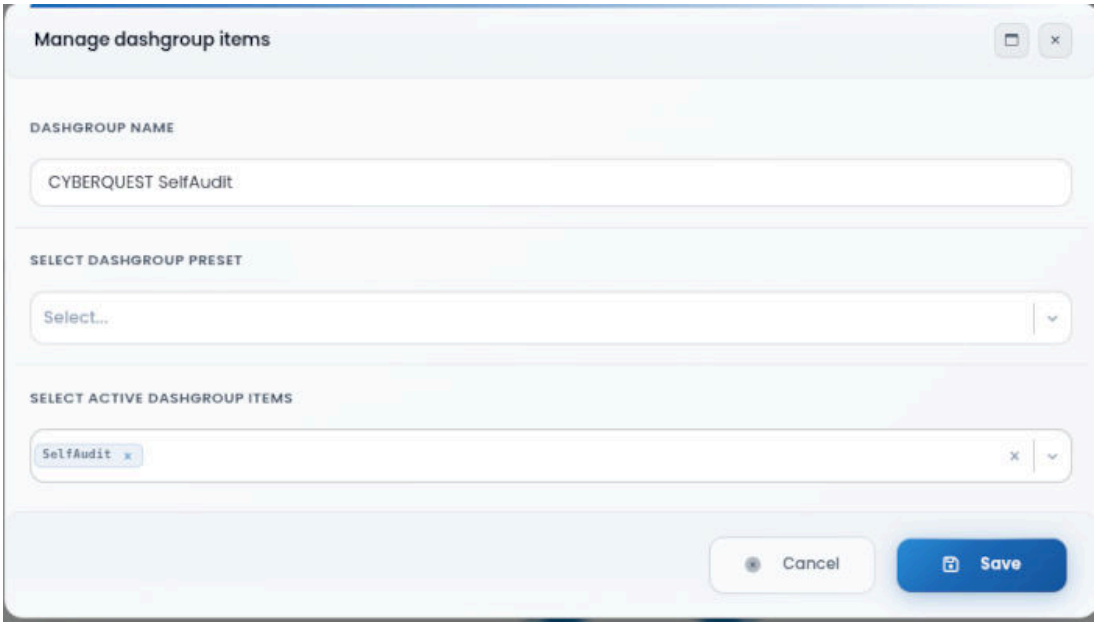
Complete the form

Fill in the form with the appropriate information, then click the Save button.

Dashgroup name: The name assigned to the new dashgroup;

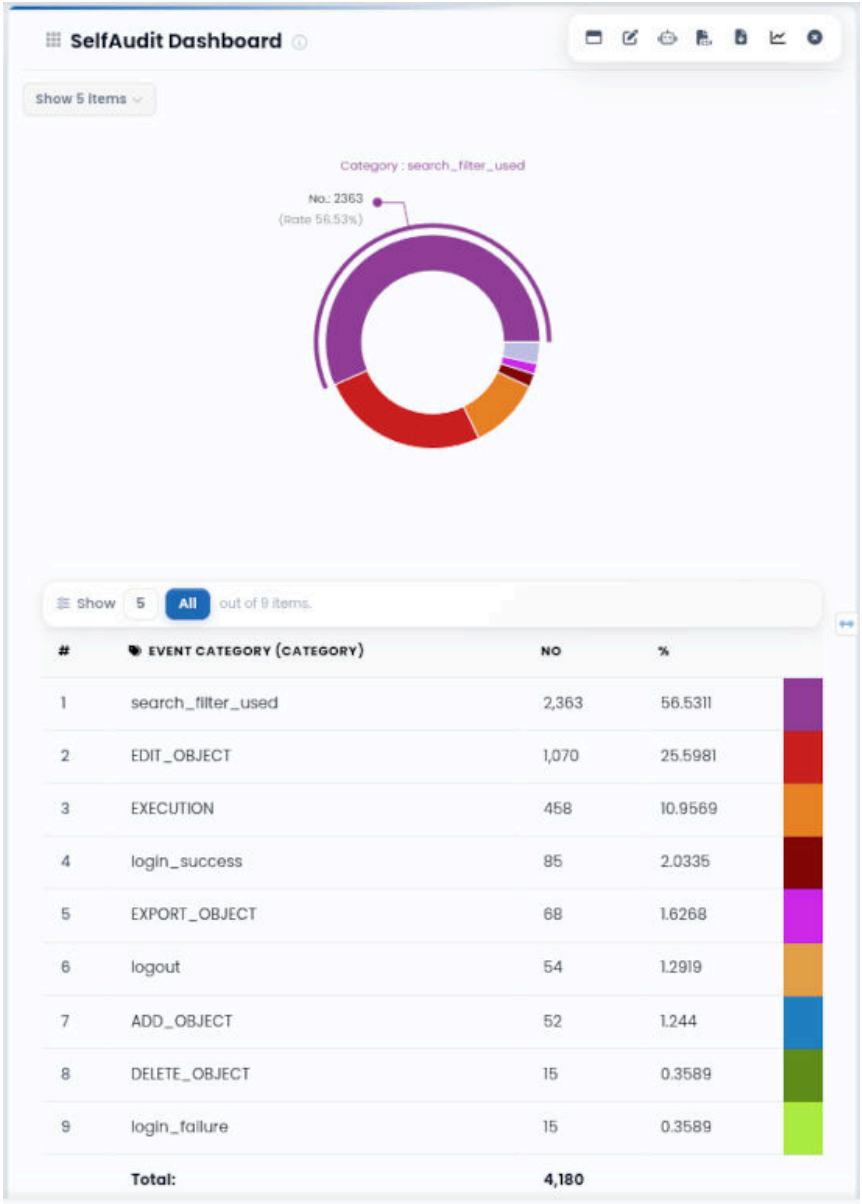
**Select dashgroup preset: **Choose from a list of existing dashgroup presets.

Select active dashgroup items: Select the items to be included in the active dashgroup from the list.



How to view data from a dashboard

The previously created item can be viewed on the **"Dashboards"** page.



This dashboard includes a set of quick action buttons:

Maximize/Minimize - Expands the dashboard to fill the entire display area or shrinks it back to its original size.

Export to CSV - Saves a CSV file containing all events displayed in the dashboard.

Export Dashboard Object - Exports the dashboard's definition in a proprietary format.

Graph selection - Opens a drop-down menu of available graphical formats for the dashboard, allowing quick changes to the display type. Note that changing the format here does not modify the dashboard definition, the change will revert upon the next load.

Edit dashboard - Enables editing and permanent modification of the dashboard's definition.

Show items - Allows adjustment of the maximum number of entries displayed in the dashboard. Since the dashboard provides a real-time overview, the number of displayed events is limited to ensure quick performance.

How to export data from dashgroup

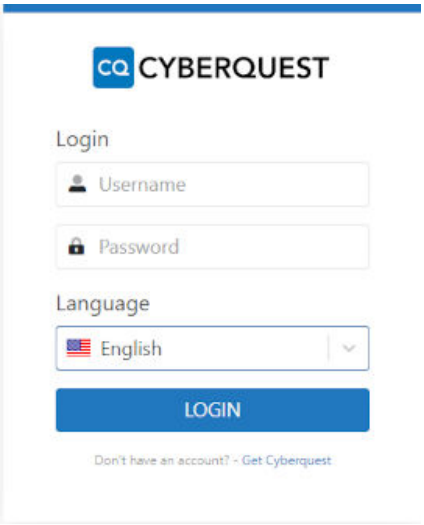
When exporting data from dashgroups, you can download a graphical report based on aggregated events or alerts.

The data export options include:

Authentication

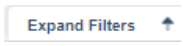
To access Web Interface, open a web browser and type the application's address or DNS name. The default address initially assigned to Web Interface is ***https://CyberquestIPAddress*** (example).

The browser automatically redirects you to CYBERQUEST's authentication page:

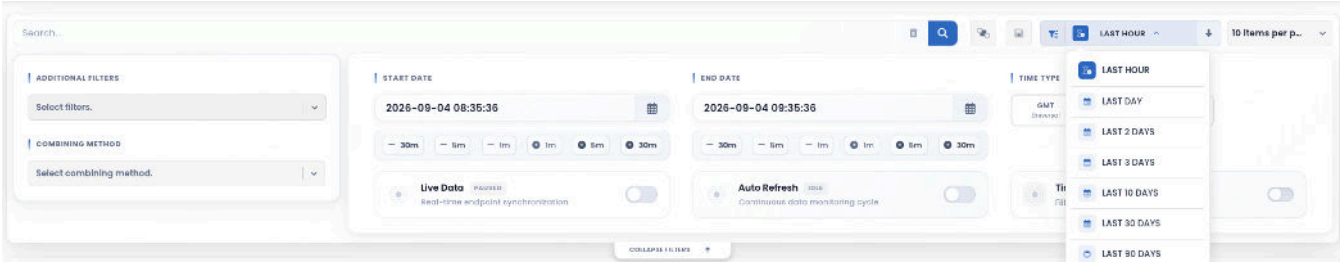


Navigate to Dashboards

- Navigate to the "**Dashboards**" page, click the

  button, and select a time interval:



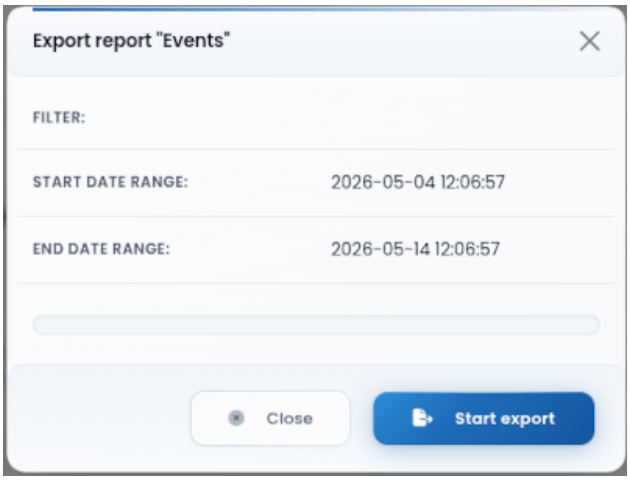
- Select the dashgroup to export (e.g., Events, Network, Alerts) or create a custom dashgroup.
- Export a dashgroup with applied filters using search and additional criteria like specific EventID, UserName, Computer, etc.

To export data from a dashgroup, click **Actions**, then select **Export** from the drop-down menu.

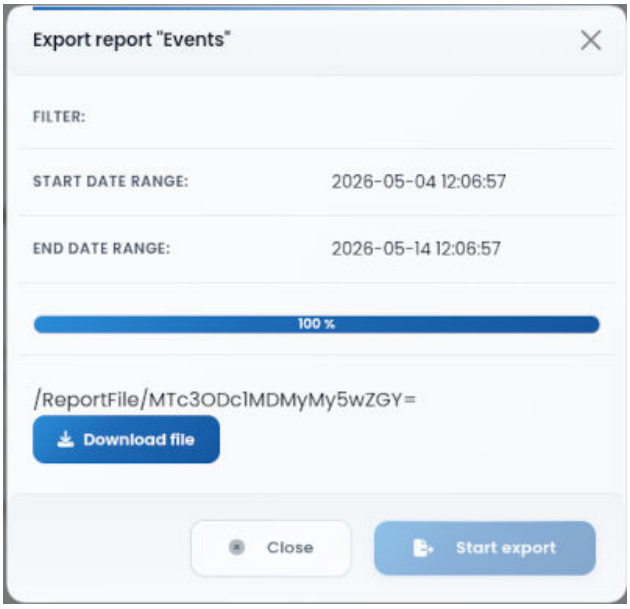


Export the Dashgroup / Generate a statistics report

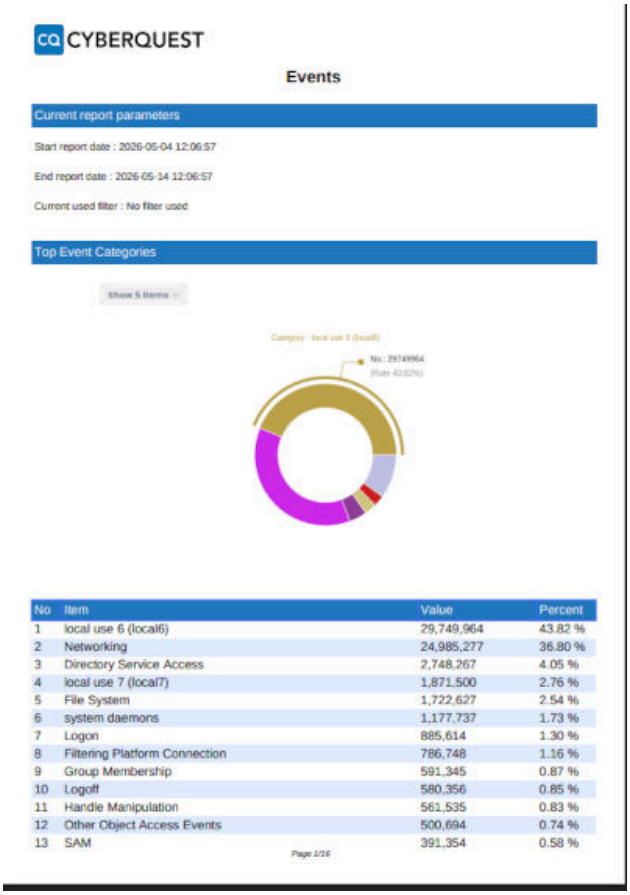
Start the export by clicking the "**Start export**" button, or cancel the operation by clicking the **Close** button.



After the export is complete, click the **Download file** button to save the report to the local machine. The report is in PDF format.



Examples of downloaded graphical dashgroup reports:



CYBERQUEST

Events

Current report parameters

Start report date : 2026-05-04 12:06:57

End report date : 2026-05-14 12:06:57

Current used filter : No filter used

Top Event Categories

No	Item	Value	Percent
1	local use 6 (local6)	29,749,964	43.82 %
2	Networking	24,985,277	36.80 %
3	Directory Service Access	2,748,267	4.05 %
4	local use 7 (local7)	1,871,500	2.76 %
5	File System	1,722,627	2.54 %
6	system daemons	1,177,737	1.73 %
7	Logon	885,614	1.30 %
8	Filtering Platform Connection	786,748	1.16 %
9	Group Membership	591,345	0.87 %
10	Logoff	580,356	0.85 %
11	Handle Manipulation	561,535	0.83 %
12	Other Object Access Events	500,694	0.74 %
13	SAM	391,354	0.58 %

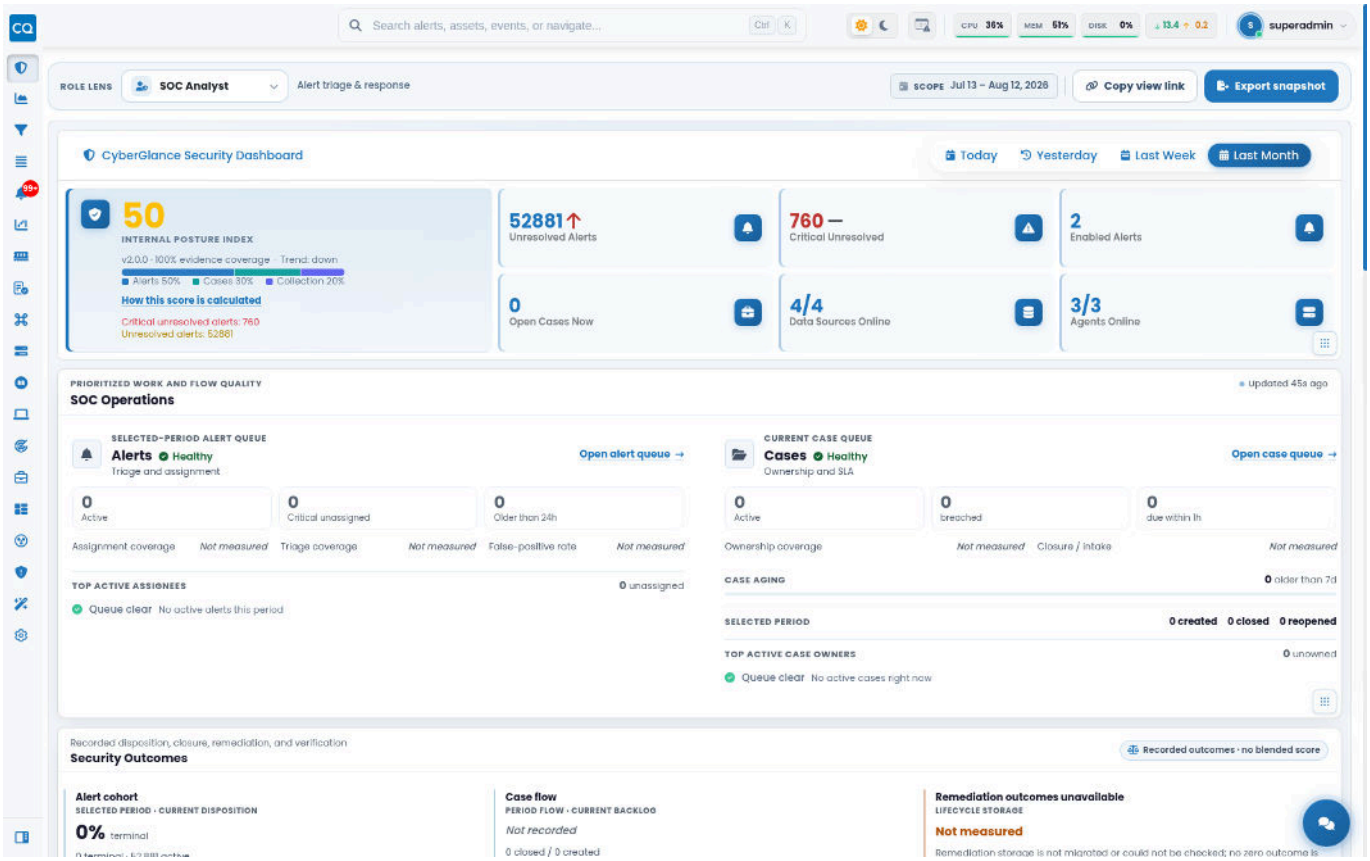
CyberGlance

What CyberGlance shows

CyberGlance is the single-screen view of where security stands right now. It brings the posture index, the alert and case queues, event volume, vulnerability exposure and platform health together, so you can read the state of the environment without opening each module in turn.

What appears on the screen depends on two things: the **role lens** you select, which decides which widgets are laid out, and the **period** you select, which decides what they count.

To open it, choose **CyberGlance** from the left-side navigation menu. The page is protected by the **view_dashboards** permission.



Select the analysis period

Use the period controls in the upper-right corner of the **CyberGlance Security Dashboard** to define the time window used for the dashboard analysis.

Four predefined periods are available:

- **Today** - shows data for the current day.
- **Yesterday** - shows data for the previous day.
- **Last Week** - shows data for the previous week.
- **Last Month** - shows data for the previous month.

The currently selected period is highlighted in the period selector. In the example above, **Last Month** is selected.

The corresponding date range is displayed in the **Scope** field at the top of the page. For example:

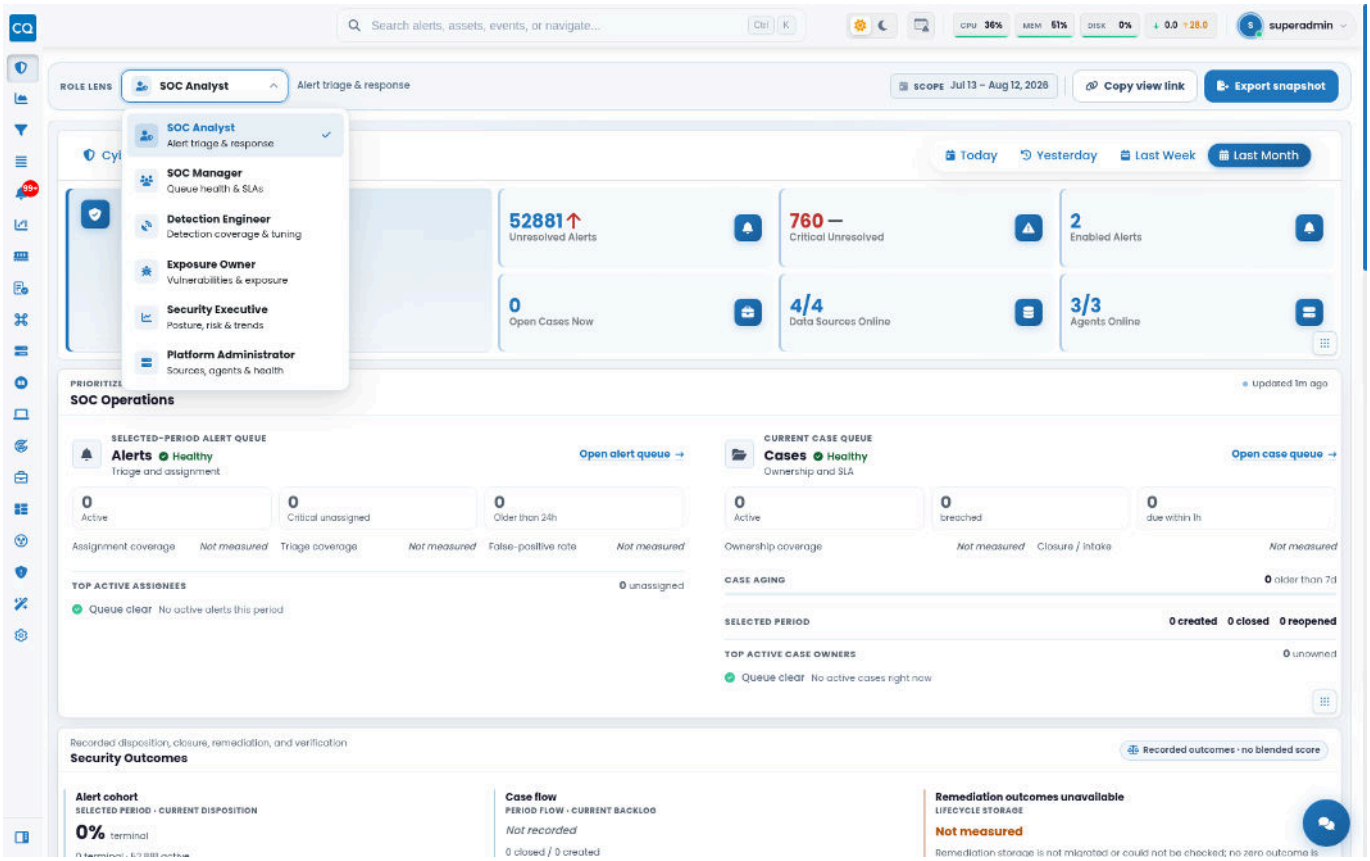
```
Jul 13 – Aug 12, 2026
```

The selected time window determines the data evaluated by the dashboard, including alert activity, detection engineering metrics, trends, and other period-based indicators.

Select a different period at any time to recalculate the dashboard for that time window.

View the dashboard by role

The **Role Lens** selector lets you adapt the CyberGlance dashboard to a specific operational perspective.



Each lens focuses the dashboard on the information most relevant to that role:

Lens	Focus
SOC Analyst	Alert triage & response
SOC Manager	Queue health & SLAs
Detection Engineer	Detection coverage & tuning
Exposure Owner	Vulnerabilities & exposure
Security Executive	Posture, risk & trends
Platform Administrator	Sources, agents & health

Dashboard layouts are independent for each Role Lens. Rearranging widgets in one lens does not change the layout of the others, allowing each role view to be customized separately.

Understanding the dashboard header

The dashboard header provides a high-level view of the current security posture and key operational indicators.

The **Internal Posture Index** is the main posture score. It is calculated from three components — **Alerts**, **Cases**, and **Collection** - using the weights displayed beneath the score. The same area also shows the model version, **evidence coverage**, and the current **Trend**.

Select **How this score is calculated** to view the values and components contributing to the score.

Two details are important when interpreting the index:

- **Unavailable components are not treated as zero.** If a component cannot be evaluated, its weight is redistributed across the components that are available. This prevents missing evidence from automatically lowering the score.
- **Evidence coverage indicates how complete the assessment is.** It helps distinguish a score calculated from complete evidence from one based on only part of the available data.

Next to the index, the KPI tiles summarize important security and operational information: **Unresolved Alerts**, **Critical Unresolved**, **Enabled Alerts**, **Open Cases Now**, **Data Sources Online**, and **Agents Online**.

Some indicators are calculated for the selected **Scope**, while others represent the current state of the environment. Period-based values change when the selected period changes. Current-state indicators, such as **Open Cases Now**, **Data Sources Online**, and **Agents Online**, reflect the status at the time the dashboard is viewed.

The widgets

Each **Role Lens** displays a selection of widgets relevant to that role. Widgets are shown only when the corresponding capability is available to the account. For example, if vulnerability data is not available, vulnerability-related widgets are not displayed rather than appearing empty.

Widget	Shows	Capability
SOC Operations	Alert and case queues side by side: active, critical unassigned, older than 24h, ownership and SLA breaches	Alerts or Cases
Security Outcomes	Recorded disposition, closure, remediation and verification for the period	Alerts, Cases or Vulnerabilities
Detection Engineering	Detection coverage and tuning signal	Alerts
Risk Convergence	Where alert, UEBA and vulnerability risk overlap on the same entity	At least two of Alerts, UEBA, Vulnerabilities
Alert Trend by Severity	Alert volume over the period, split by severity	Alerts
Alert Status Distribution	The split across alert statuses	Alerts
Top Alert Types	The most frequent alert names	Alerts
Latest Critical Alerts	The most recent high-severity alerts	Alerts
Top Affected Entities	The users, computers and addresses named most often	Alerts
Case Aging	How long open cases have been open	Cases
Event KPIs / **Event Trend**	Event volume and its movement over the period	Events
Events by Category / **Top Event Sources**	Where the events are coming from	Events
Vulnerability Exposure	Exposure and its lifecycle	Vulnerabilities
UEBA Risk Leaders	The highest-risk entities by behaviour	UEBA
Anomaly Hotspots	Where anomalies are concentrated	UEBA
Integration Health	The state of configured integrations	Integrations

Widgets that track data freshness also show when their information was last updated. This helps distinguish a widget with **stale data** from one that is simply reporting little or no activity.

Drilling into the data

CyberGlance widgets provide direct access to the underlying data. Selecting a value opens the corresponding module - such as **Alerts**, **Cases**, or **Browser** - with the relevant context applied.

Depending on the widget, the drill-down can include the selected entity, severity, status, or other relevant value, together with the current **Scope**.

This keeps the destination focused on the data represented by the selected dashboard element and within the same analysis period.

The destination indicates when the view has been opened from **CyberGlance** and when filters have been applied.

Sharing and exporting a view

Two actions are available in the upper-right corner of the dashboard.

Copy view link copies a link containing the current **Role Lens** and selected period. Opening the link restores the same CyberGlance context, subject to the permissions of the user accessing it.

Export snapshot downloads the current dashboard data as a JSON file. The exported data can be used as supporting information for reports, investigations, or cases.

Customizing the layout

Widgets can be repositioned by dragging them and resized using the control in the bottom-right corner.

Each **Role Lens** maintains its own layout, so changes made in one lens do not affect the arrangement of widgets in another.

The dashboard is responsive and automatically adjusts the widget layout to the available screen width.

Interpreting dashboard data

When reviewing CyberGlance, consider both the selected **Scope** and the availability of the underlying data.

The Scope defines the analysis period. Period-based widgets use the date range displayed in **Scope**. Changing the selected period updates these widgets using data from the corresponding interval.

No results do not necessarily indicate a problem. A widget may have no relevant data for the selected period. Where applicable, CyberGlance displays states such as *Queue clear*, *No active alerts this period*, or *Not measured* to distinguish the absence of activity or evidence from an error.

Not measured is different from zero. Some indicators depend on information recorded during operational workflows, such as closure outcomes, remediation, or verification. If the required information is unavailable, CyberGlance reports **Not measured** rather than treating the result as zero.

Current-state indicators are independent of the selected period. Indicators such as **Open Cases Now**, **Data Sources Online**, and **Agents Online** represent the current state of the environment, while period-based indicators are calculated using the selected **Scope**.

Permissions

Access to CyberGlance requires the `**view_dashboards**` permission.

Individual widgets are displayed according to the capabilities and data available to the account. Drill-down destinations remain subject to the permissions required by their corresponding modules.

Reports Module

Introduction to Reports module

The Reports module provides access to predefined and customizable reports, enabling scheduled and ad hoc generation of compliance and operational summaries through an intuitive web interface.

The **Reports** module can be accessed by clicking the



button, located in the left section of the Web Interface.

In addition to opening the Reports module and interacting with the included reports as described in this chapter, the Web Interface offers a quick search feature for locating specific reports. To access the Quick Filter box, first expand the Reports tree in the left section of the interface. Then, enter the report name or part of it into the Quick Filter box located at the top-

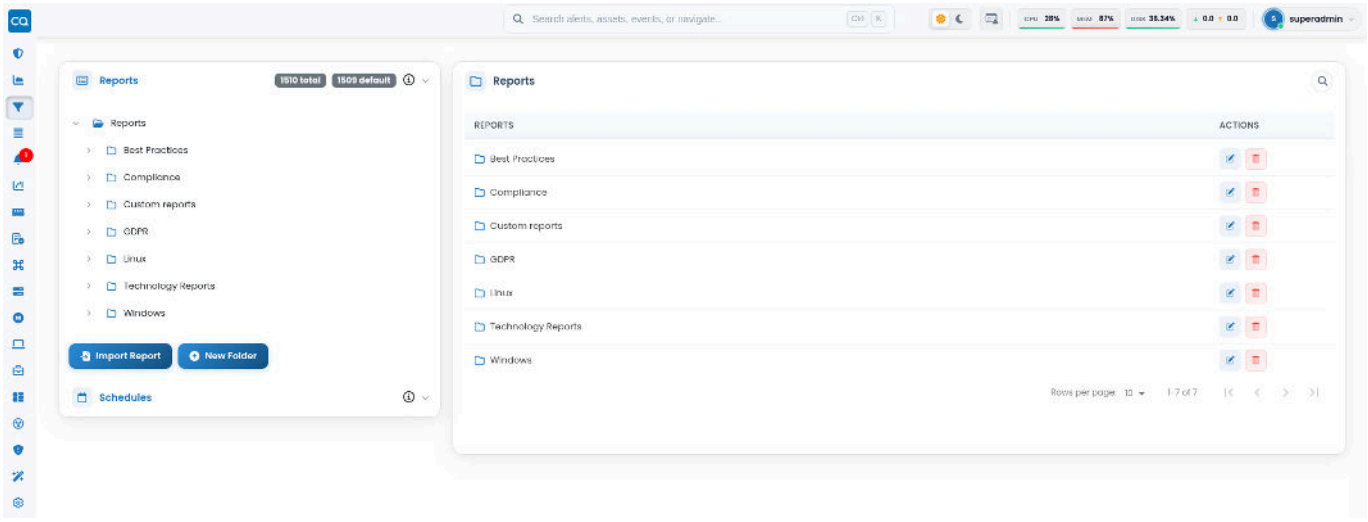
right corner of the interface.

This module supports both scheduled and ad hoc reporting-either collectively or at a granular level-providing a comprehensive compliance and operational overview of IT environments. The interface restricts report visibility based on user authorization. Through this simple, web-based interface, authorized users can quickly access predefined and customizable reports to derive actionable insights.

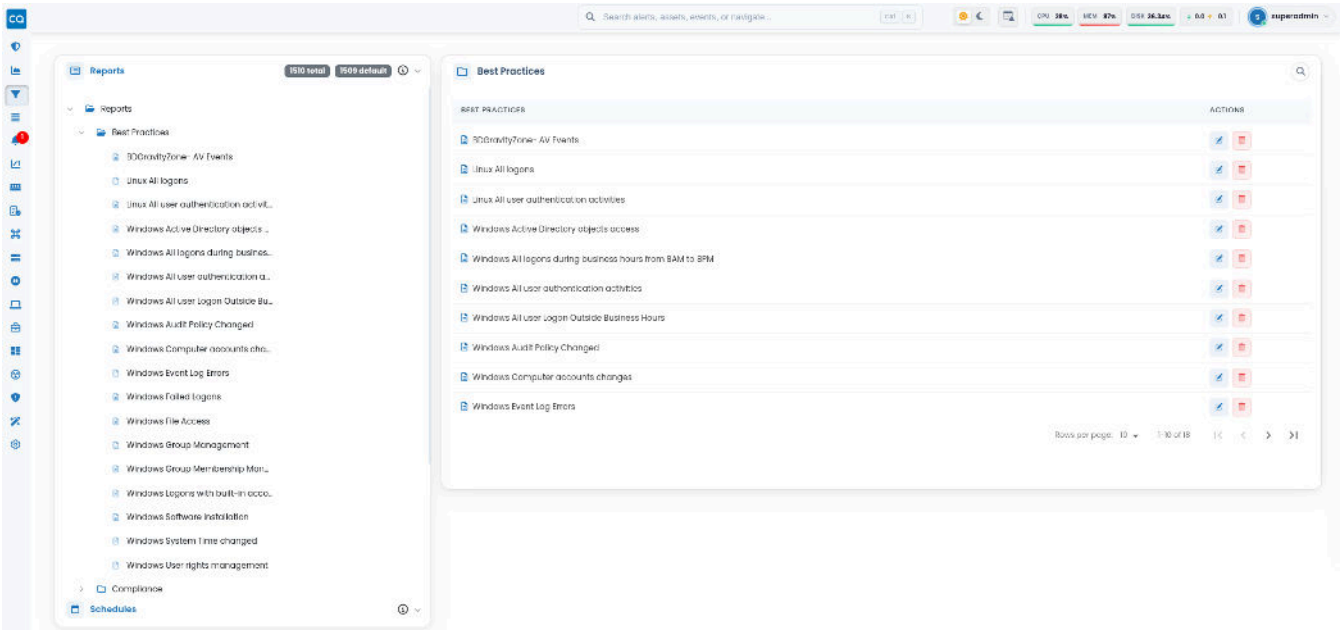
Types of Reports

Available Reports

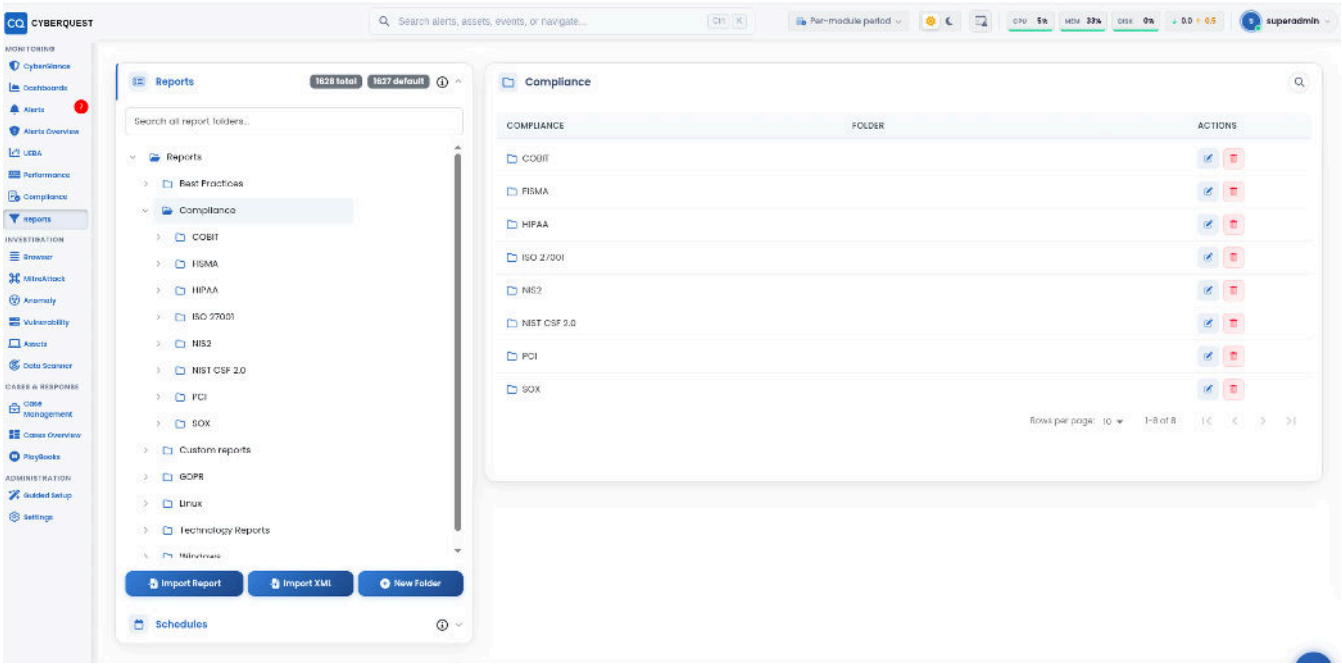
The **CYBERQUEST Reports** module includes both technological and compliance reports. CYBERQUEST provides over 1500 preconfigured reports. The report tree is structured as follows:



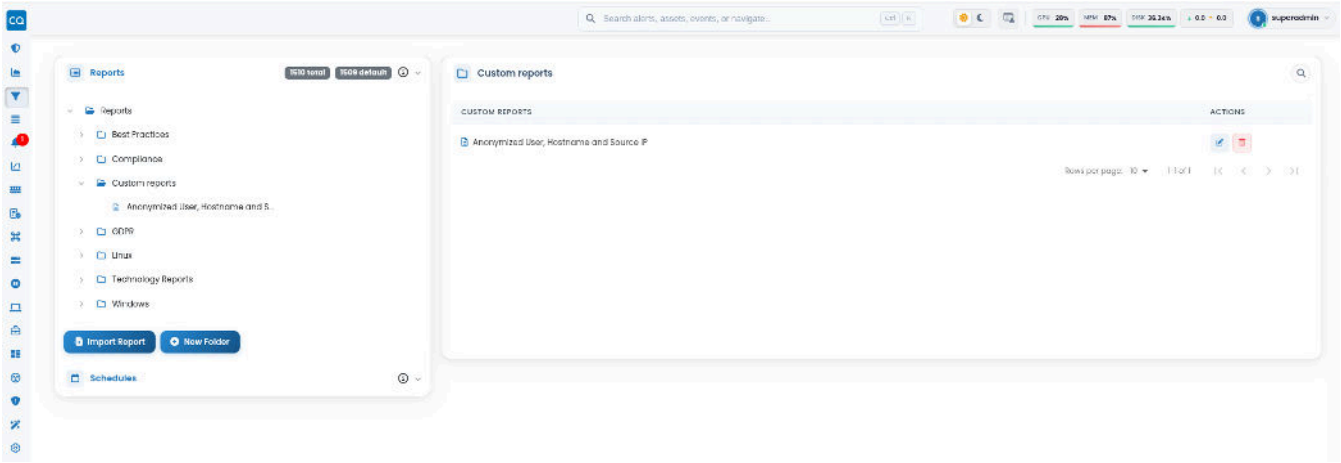
- The **Best Practices** folder contains a collection of frequently used technology reports, summarizing and detailing technology best practices commonly adopted by customers.



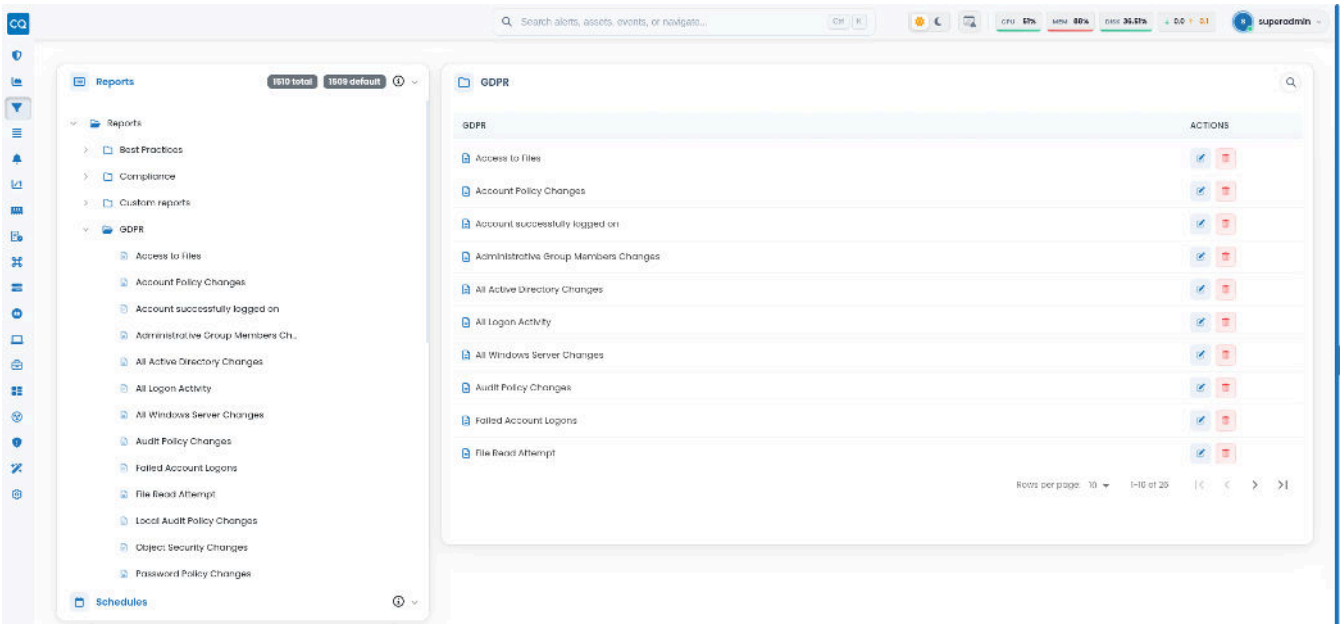
- The **Compliance** folder provides access to all reports mapped to supported compliance standards, with addressed compliance requirements listed accordingly.



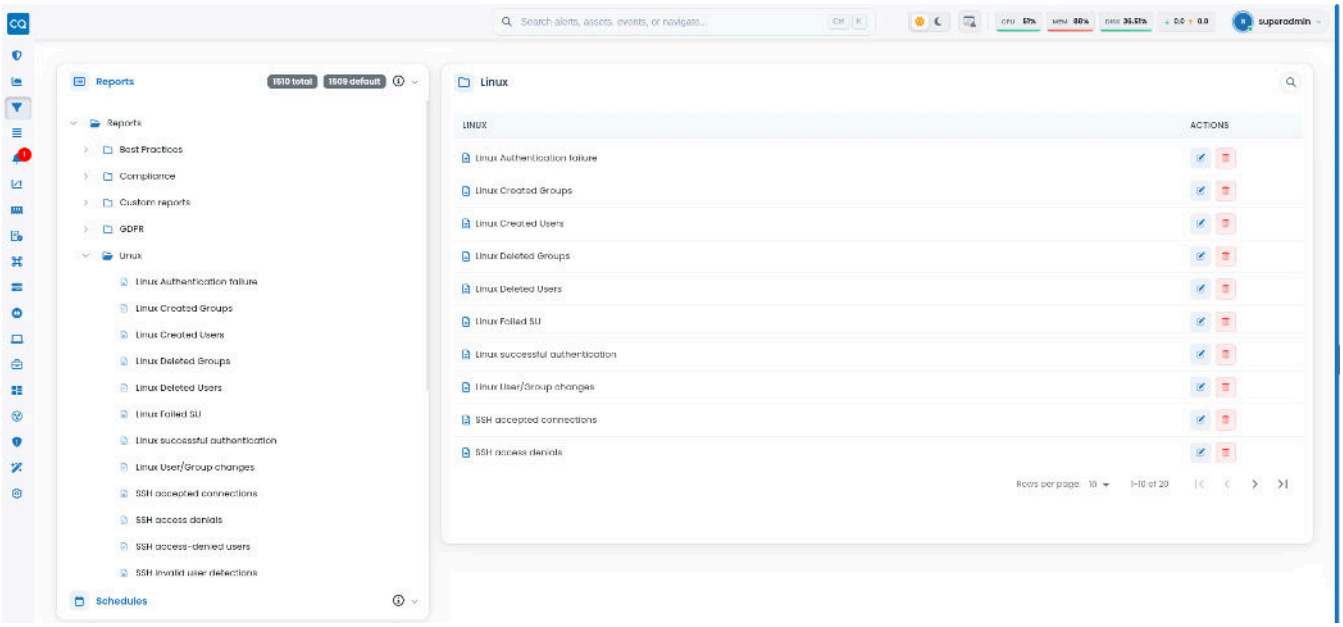
- The **Custom Reports** folder contains user-defined reports that are not included by default in CYBERQUEST.



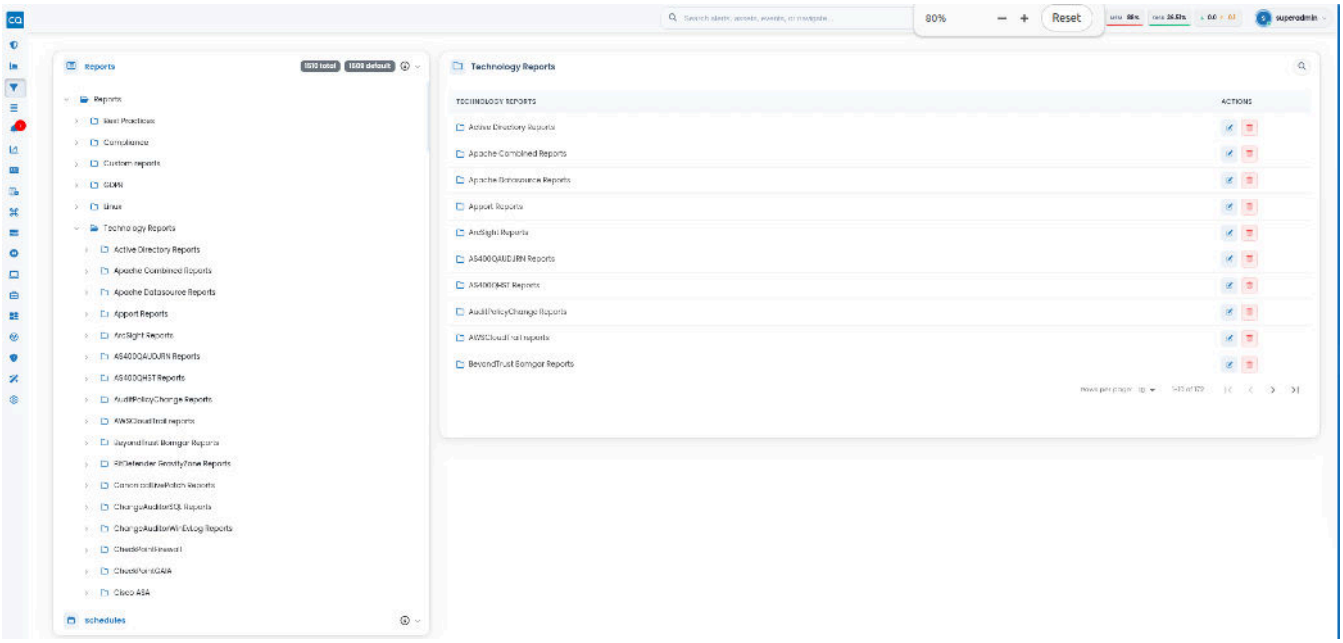
- The **GDPR** folder contains a collection of reports related to General Data Protection Regulation (GDPR) compliance.



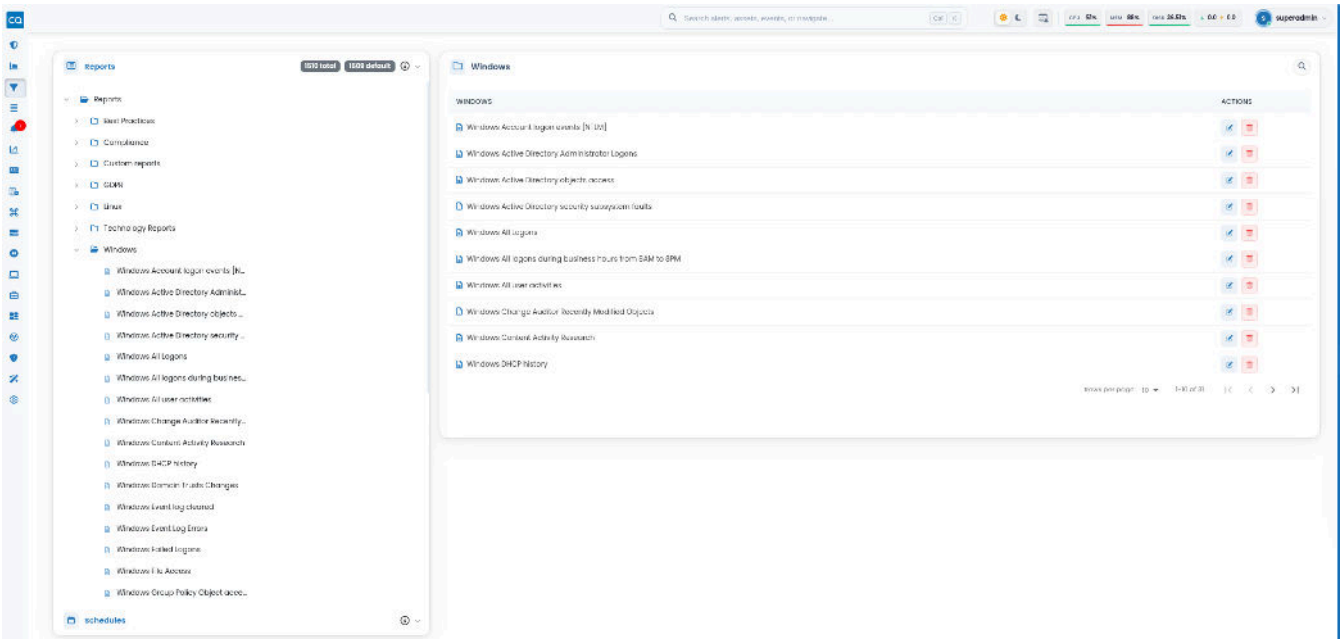
- The **Linux** folder provides access to reports specific to Linux systems.



- Each **Technology Reports** folder contains summarized and detailed reports specific to that technology, designed to assist operators in reporting on compliance-related issues.



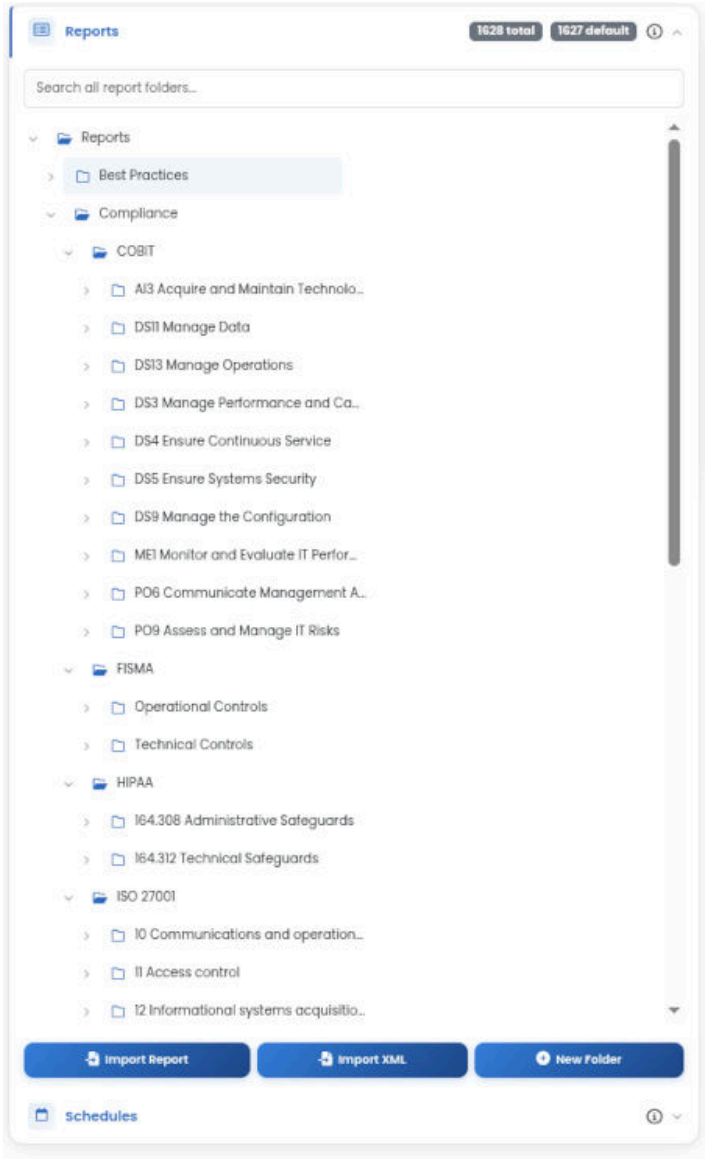
- Accessing the **Windows** folder displays a collection of reports related to Windows system activity and performance.

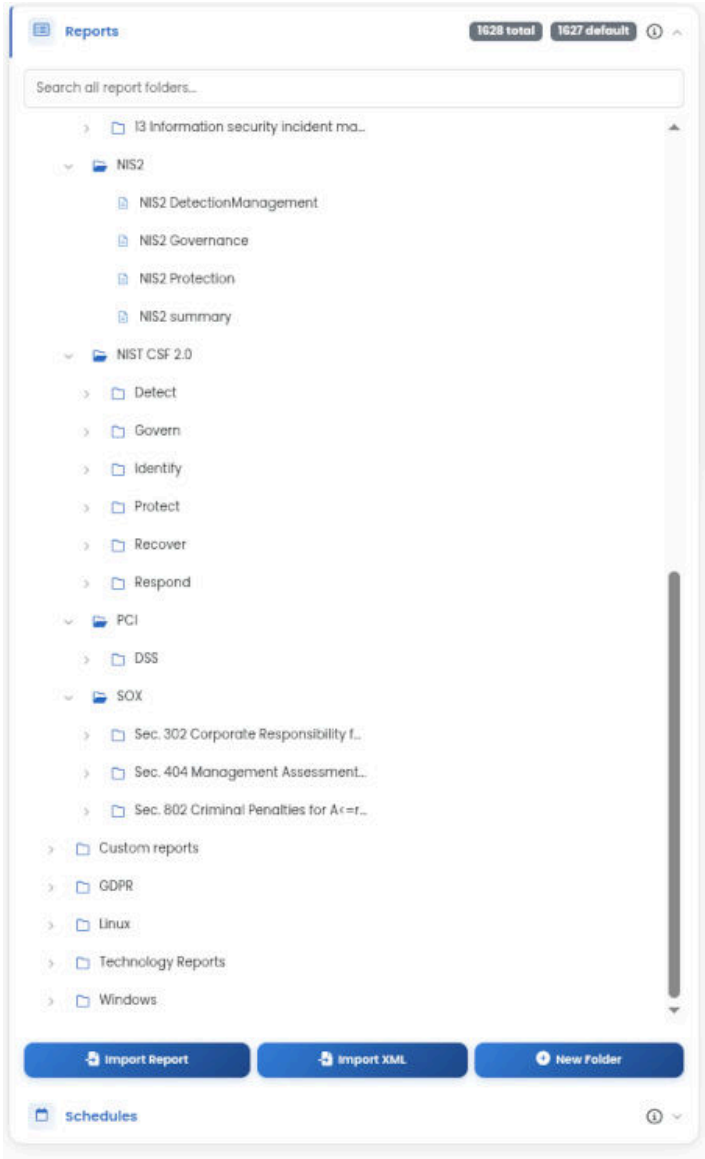


Compliance Reports

The built-in CYBERQUEST reports are designed to support compliance with the following standards:

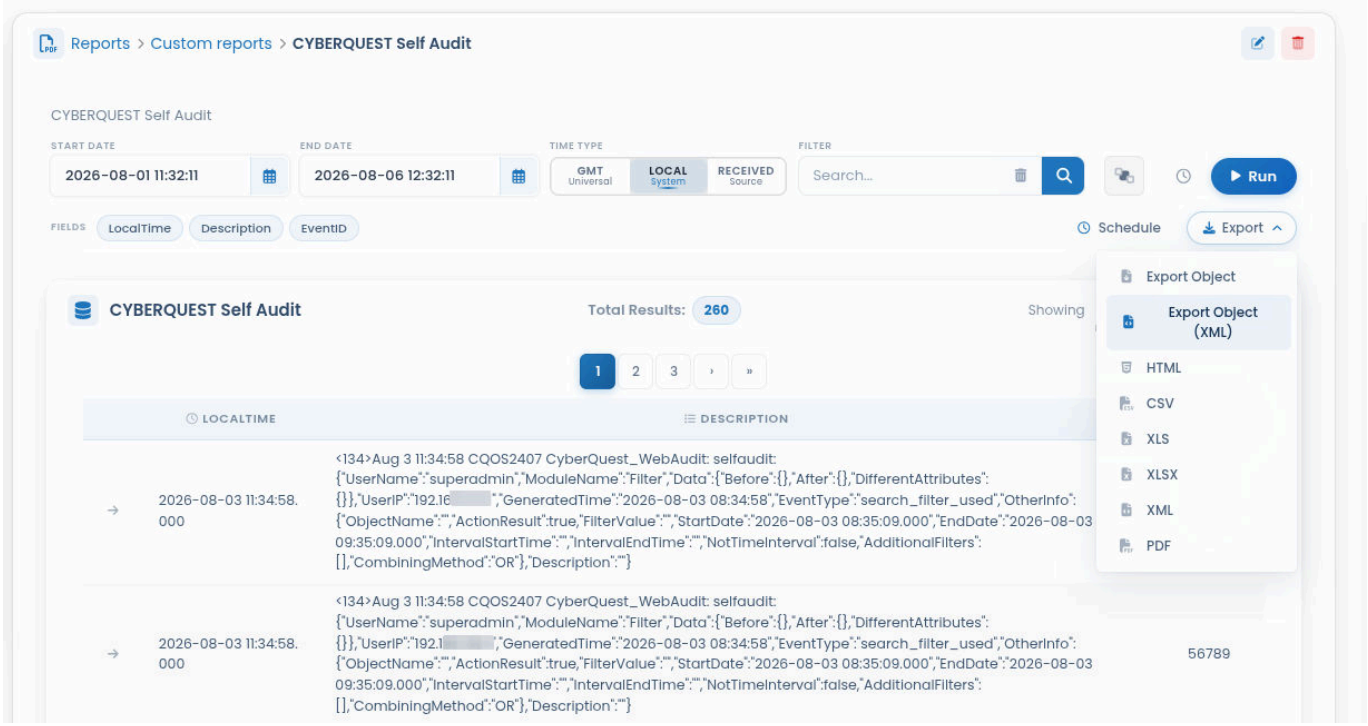
- **COBIT** (https://www.isaca.org/resources/cobit) (Control Objectives for Information and Related Technology)
- **FISMA** (https://www.cisa.gov/topics/cyber-threats-and-advisories/federal-information-security-modernization-act) (Federal Information Security Modernization Act)
- **GDPR** (https://eur-lex.europa.eu/eli/reg/2016/679/oj) (General Data Protection Regulation)
- **HIPAA** (https://www.hhs.gov/hipaa/index.html) (Health Insurance Portability and Accountability Act)
- **ISO 27001** (https://www.iso.org/standard/27001) (Information Security Standard)
- **NIS2** (https://eur-lex.europa.eu/eli/dir/2022/2555/oj) (Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union)
- **NIST CSF 2.0** (https://www.nist.gov/cyberframework) (NIST Cybersecurity Framework 2.0)
- **PCI DSS** (https://www.pcisecuritystandards.org/standards/pci-dss/) (Payment Card Industry Data Security Standard)
- **SOX** (https://www.govinfo.gov/app/details/PLAW-107publ204) (Sarbanes-Oxley Act of 2002)


Reports
1628 total
1627 default
Search all report folders...
Reports
Best Practices
Compliance
COBIT
AI3 Acquire and Maintain Technolo...
DS11 Manage Data
DS13 Manage Operations
DS3 Manage Performance and Ca...
DS4 Ensure Continuous Service
DS5 Ensure Systems Security
DS9 Manage the Configuration
ME1 Monitor and Evaluate IT Perfor...
PO6 Communicate Management A...
PO9 Assess and Manage IT Risks
FISMA
Operational Controls
Technical Controls
HIPAA
164.308 Administrative Safeguards
164.312 Technical Safeguards
ISO 27001
10 Communications and operation...
11 Access control
12 Informational systems acquisitio...
Import Report
Import XML
New Folder
schedules



Managing Reports

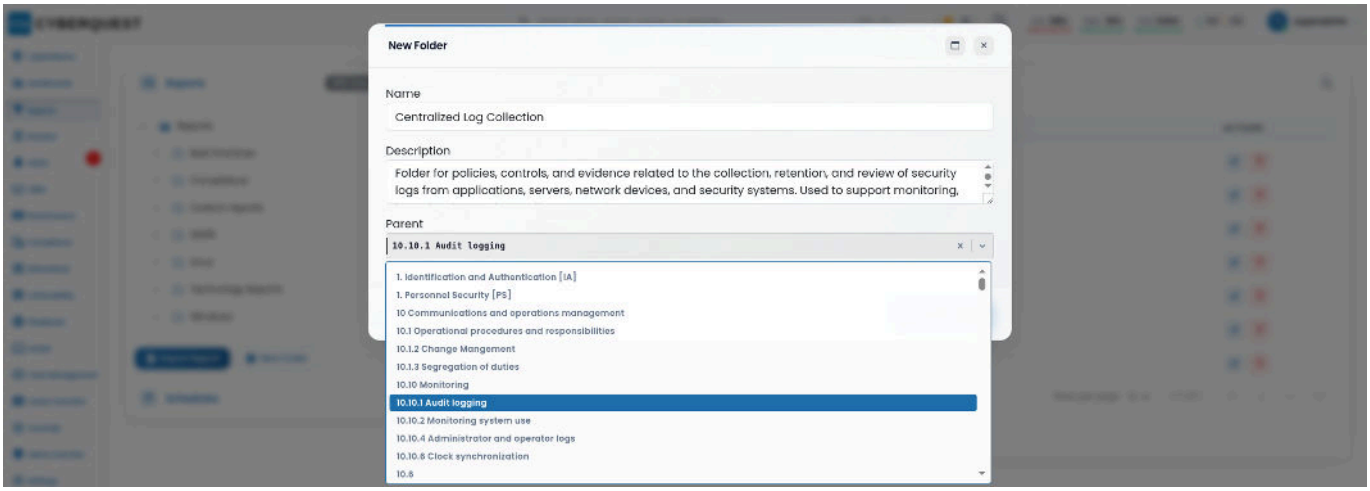
To create, edit, or delete a folder, access the **Reports** module from the Web Interface. The following window will open:



- To create a new folder, click the

  New Folder

  button. The following page will open:



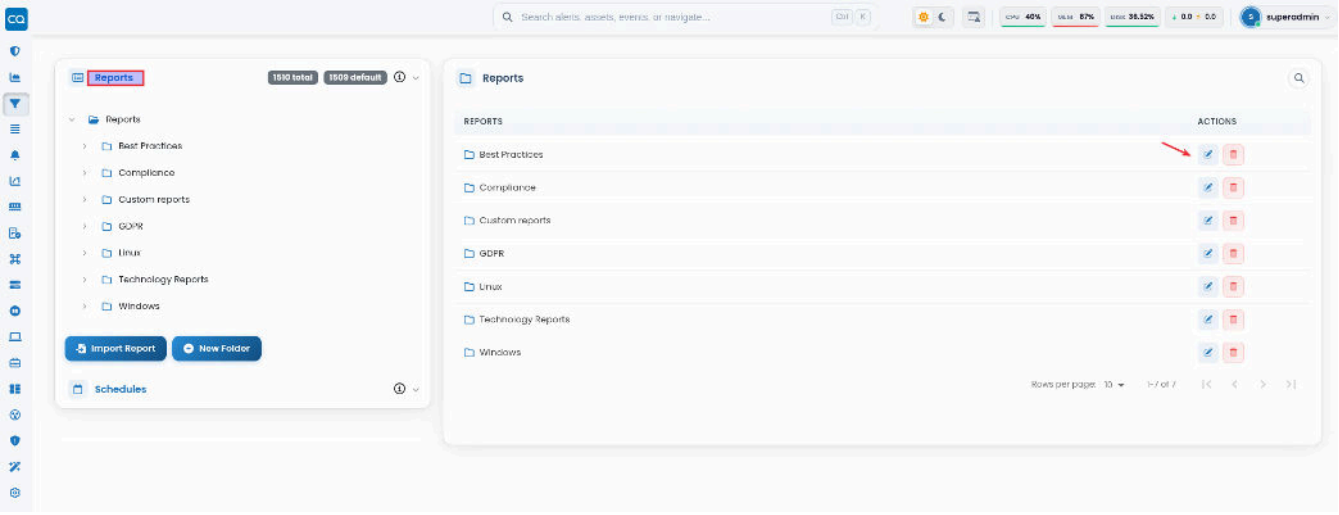
Name: Enter the name of the new folder. This name will appear in the **Reports** list.

Description: Provide a description for the new folder.

Parent: Choose the location where the new folder will be added.

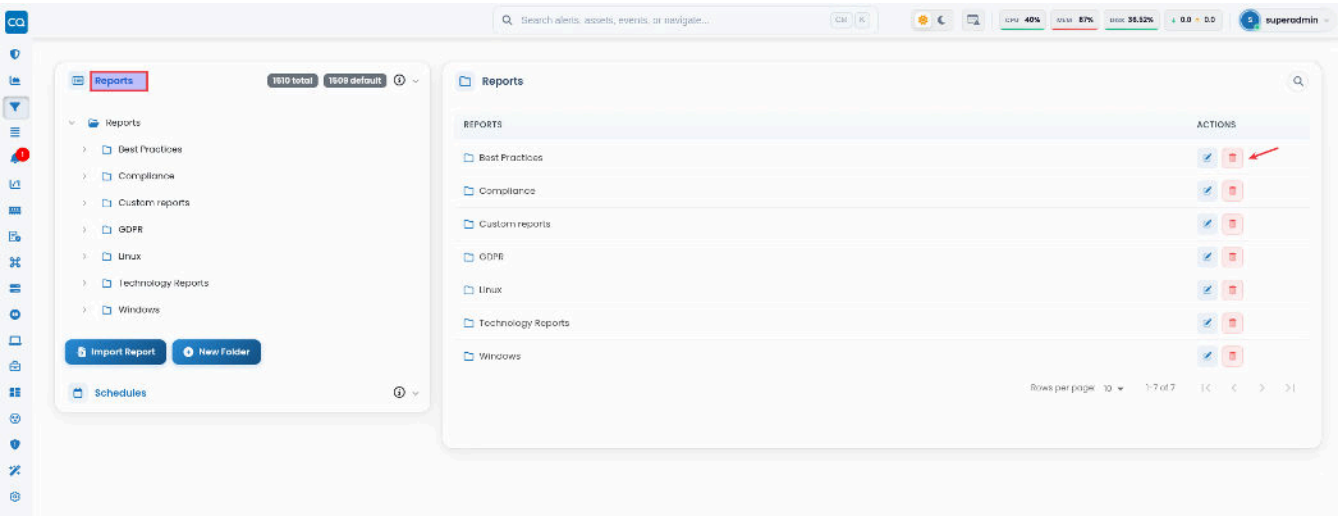
Complete the form and press “Save” button to save changes, or “Cancel” button to close the window without saving.

- To edit a folder, click on the **Reports** folder to display all available folders, then click the **Edit** icon next to the target folder.

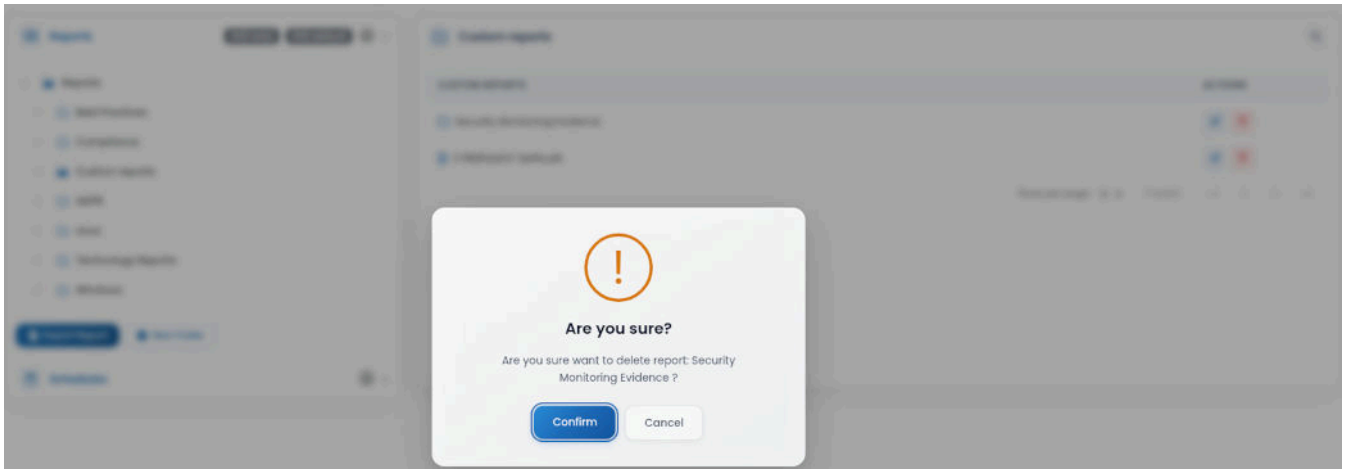


This process follows the same steps as creating a *New Folder*.

- To delete a folder, click on the **Reports** folder to display all available folders, then click the delete button:



As a precaution, a confirmation prompt will appear. Click the "***Confirm***" button to confirm the deletion, or click the "***Cancel***" button to cancel the action.



Create Custom Reports

Access the **Custom Reports** folder to view reports that are not included by default in CYBERQUEST.

Navigate to the **Browser** module, accessible upon logging into the application or at any time by clicking the



button located in the left section of the Web Interface.

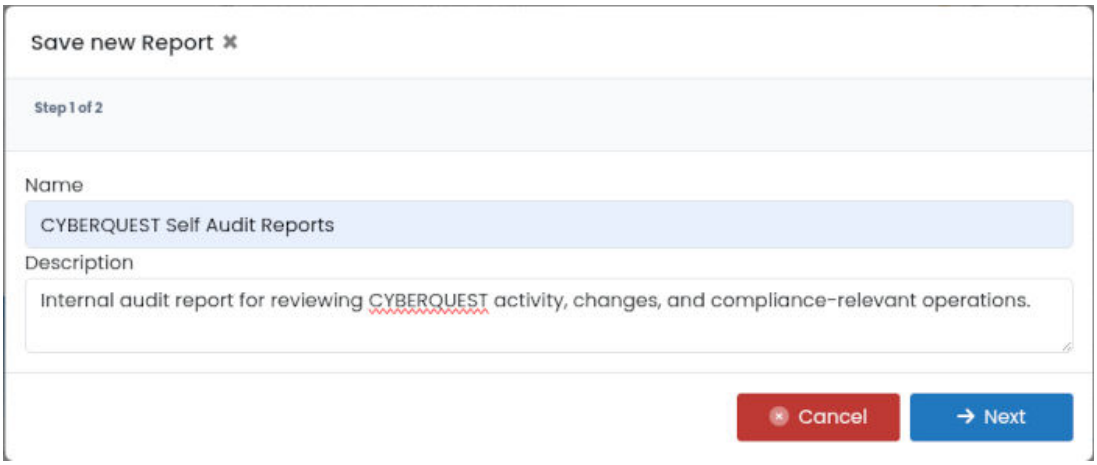
Create a filtering rule to display self-audit events using the condition **EventID:"56789"**. To save the result as a report, click **SAVE OPTIONS > Save as New Report**.

Complete the form

Complete in the form with the required information and click the "***Next***" button to proceed.

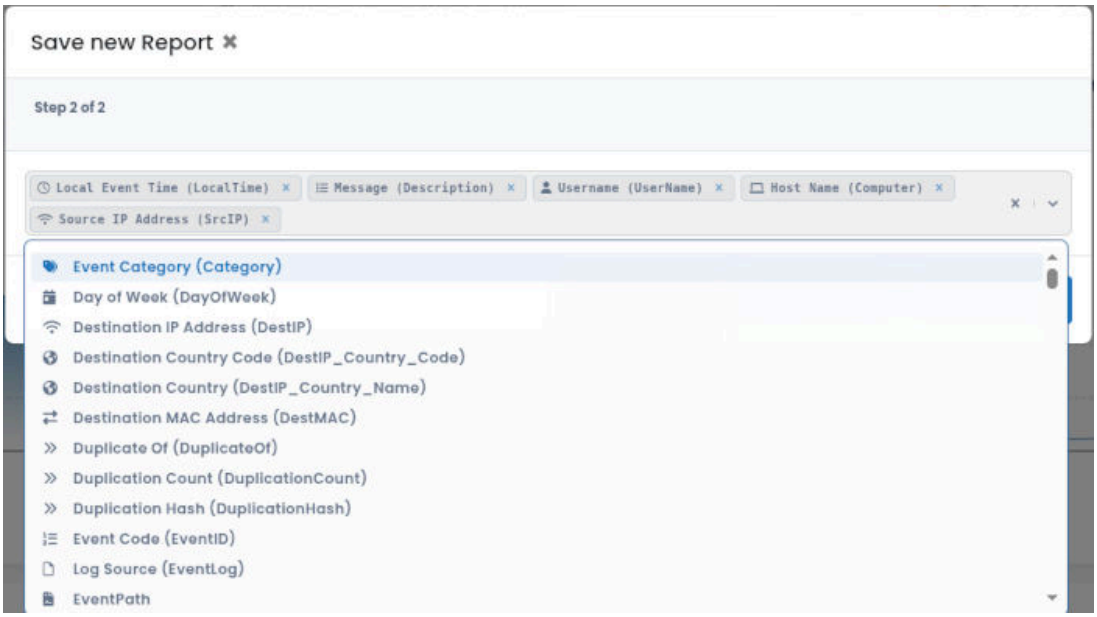
Name: The name of the new Report;

Description: Provide a description for the new report.

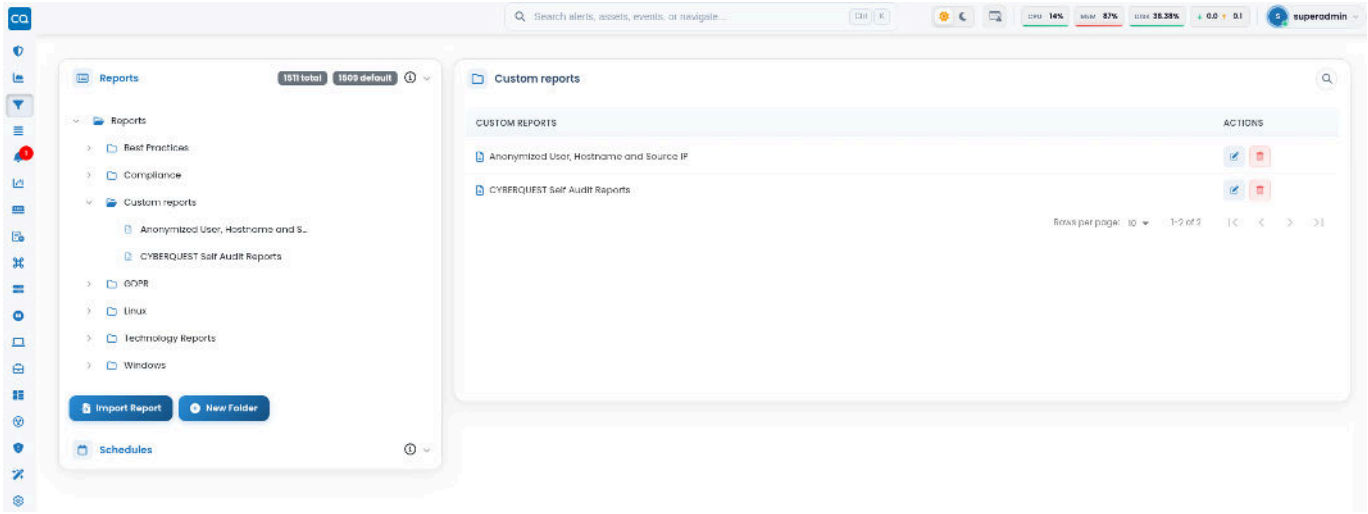


Save the reports

Choose the fields with the desired information and press the "***Save***" button.

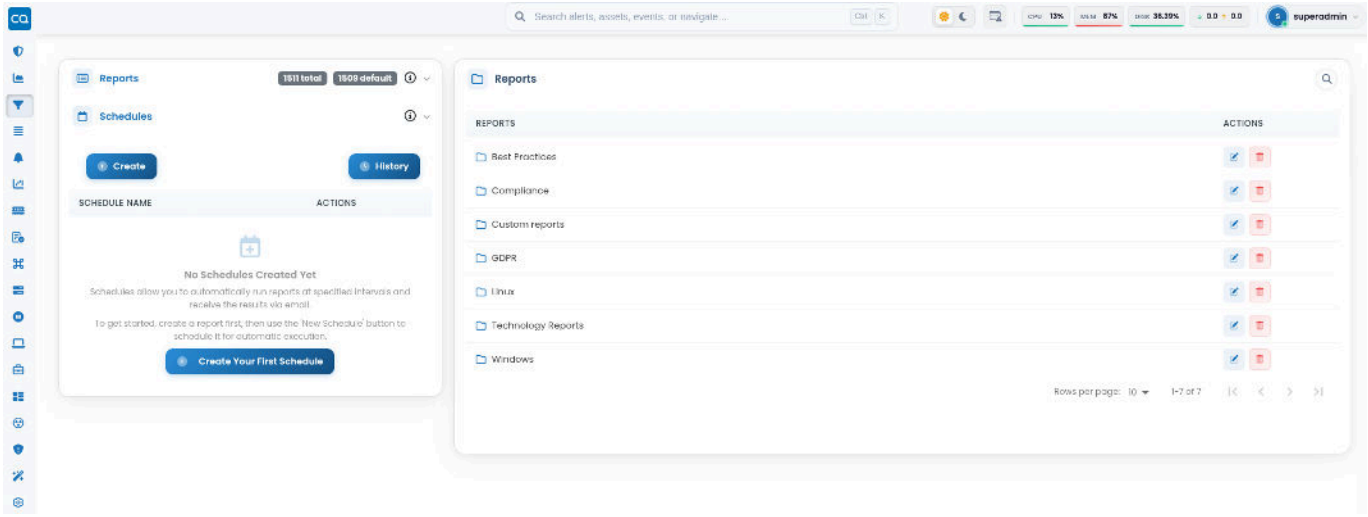


The report will be saved on the "Reports" page, in "Custom reports" folder.



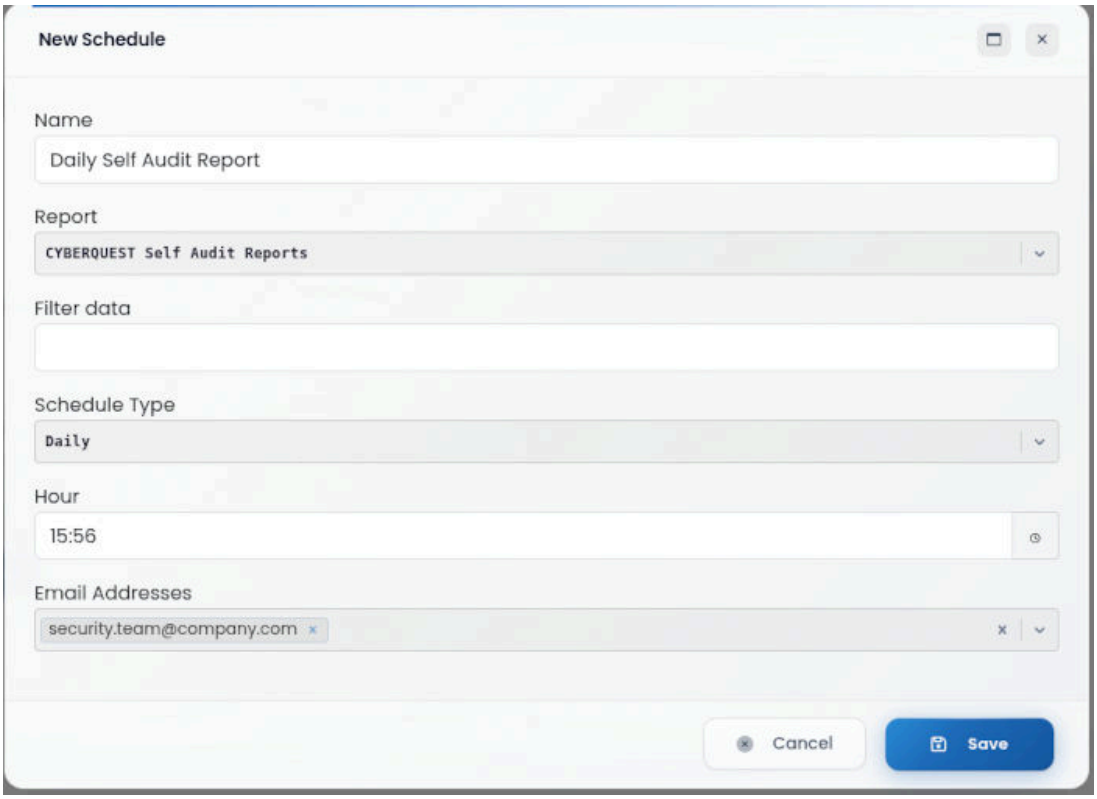
Schedule Reports

Selecting **Schedules** in the **Reports and Schedules** section of the **Reports** module displays a list of all defined report schedules.



Each listed schedule can be edited or deleted.

A new schedule can be created by clicking the "***Create***" button or "***Create Your First Schedule***" button, which opens the schedule creation window:



- **Name:** Enter a descriptive name for the scheduled report;
- **Report:** Select the source report from the available drop-down list;
- **Filter Data:** Specify a filter query to define the data included in the report;
- **Schedule Type:** Define the report generation interval by selecting Daily, Weekly, or Monthly;
- **Hour:** Set the specific time of day when the report should be generated;
- **Email Addresses**: Enter the email addresses of recipients, one per line, without punctuation separators. There is no limit to the number of recipients supported by the scheduling engine.

  Click **Save** to create the new schedule, or **Cancel** to discard the changes and return to the main interface.

Working with Reports module

Reports module interface is divided in two sections:

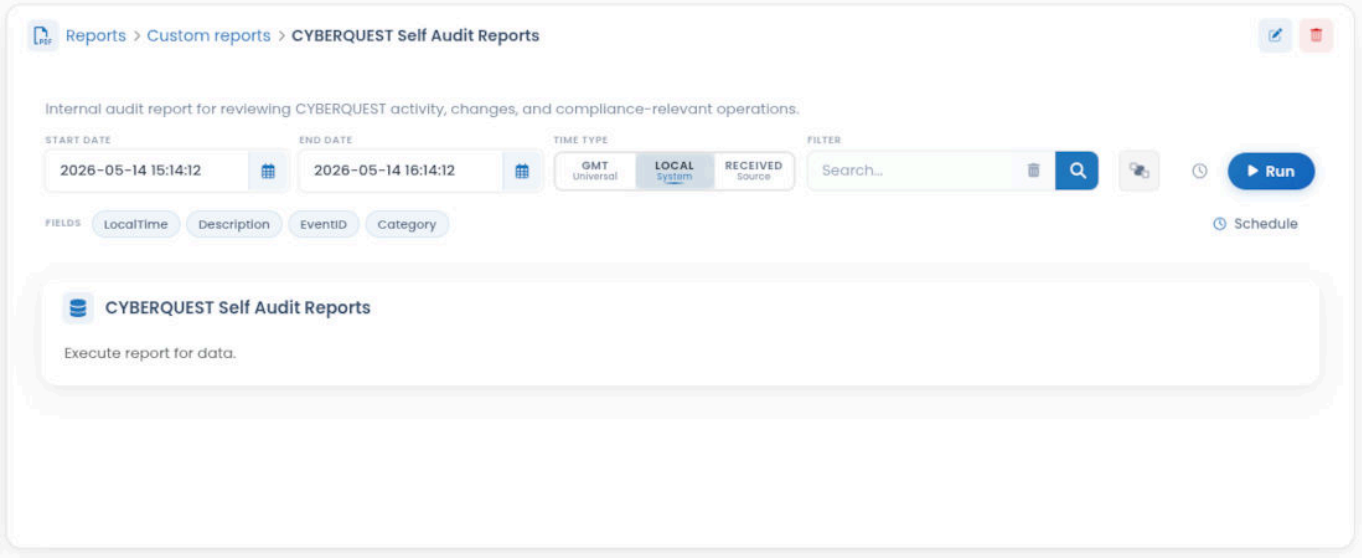
- **Reports and schedules** section allows you to navigate the reports folder structure and to select the report you want to action on, as well as creating, editing and deleting report schedules.
- **Reports detail** section allows you to edit, delete and execute a selected report.

The **Reports** module interface is divided into two main sections:

- **Reports and Schedules:** Enables navigation through the report folder structure, selection of specific reports, and management of report schedules (create, edit, delete).
- **Report Details:** Provides options to edit, delete, or execute the selected report.

Report detail window

Selecting a report from the list displays the Report Details window on the right, where the selected report can be edited, deleted, or executed.



The detail window includes the following elements:

- Report title and description located in the top-left corner, displays the full path, report name, and associated description;
- Edit

  button located in the top-right corner, used to modify the selected report;
- Delete

  button positioned next to the Edit button, used to remove the selected report;
- Run

  and Schedule

  buttons used to execute the report immediately or create a schedule from the current execution settings.

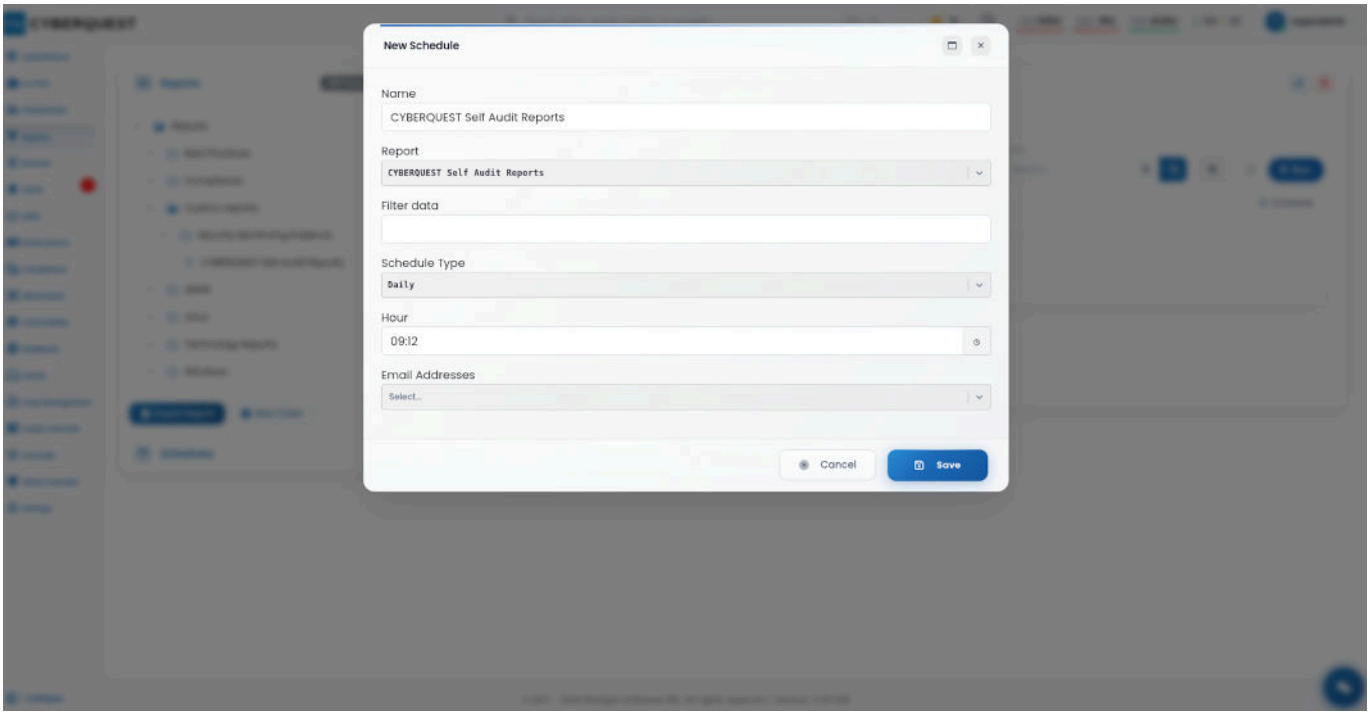
Executing reports

To execute a report, ensure that the execution options panel is visible.

Execution options allow you to control in detail what data will be included in report:

- **Start Date** and **End Date** fields define the reporting period.
- The **Items on page** drop-down menu allows selection of the number of items displayed per page (100, 50, or 10).
- Enabling the **Time Interval** checkbox allows selection of specific time ranges for each day within the selected date range.
- A time reference indicator (LocalTime, GMT, or ReceivedTime) is displayed to the right. The selected option determines how time values are interpreted in the report.
- The **Search** field accepts custom queries to limit the data included in the report. This field supports the same syntax used in the Dashboards, Browser.
- Below the Filter Data box, a field selection panel is available to customize the report columns. Additional fields can be selected or deselected as needed.
- Reports can also be scheduled with the selected execution options by clicking the

button in the details window. This opens the **Add/Edit Schedule** pop-up window:



Name: Enter a representative name for the scheduled report, or leave the default value;

Report: Displays the source report pre-selected from the main Report Details window. This can be changed using the drop-down list;

Filter Data: Contains the filtering query defined in the main Report Details window. The query can be modified as needed;

Schedule Type: Select the report execution interval (Daily, Weekly, or Monthly). Available configuration options will adjust based on the selected type;

Hour: Specify the hour at which the report should be executed;

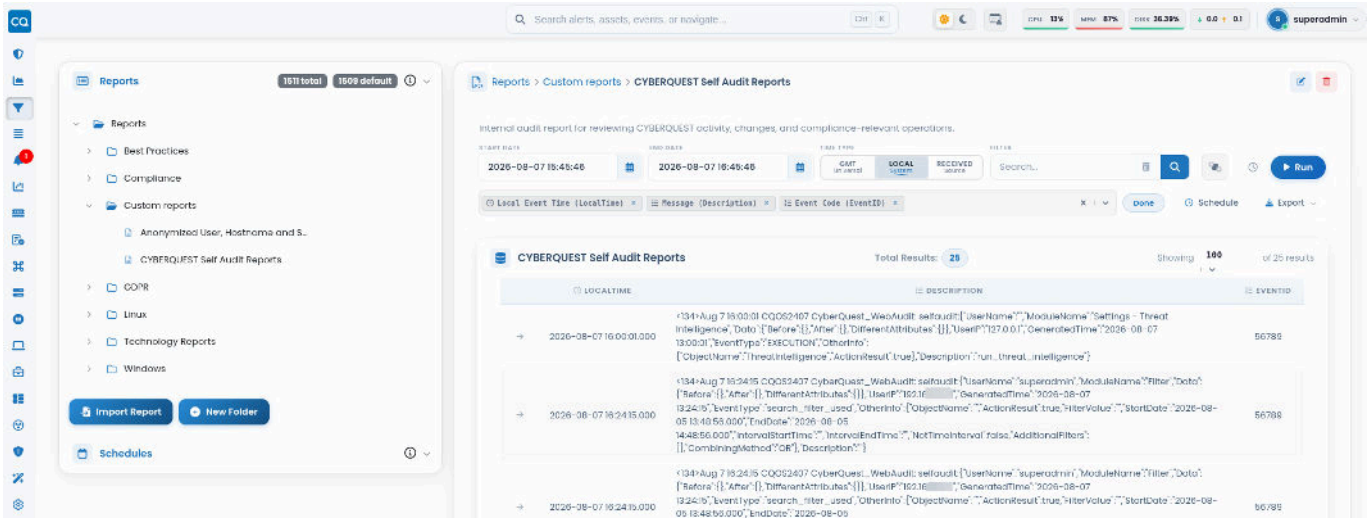
Email Addresses: Enter the email addresses of the recipients. Each address must be entered on a separate line without punctuation. There is no limit to the number of recipients supported by the scheduling engine.

Click **Save** to create the new schedule, or **Cancel** to discard the changes and return to the main interface.

In main interface, press

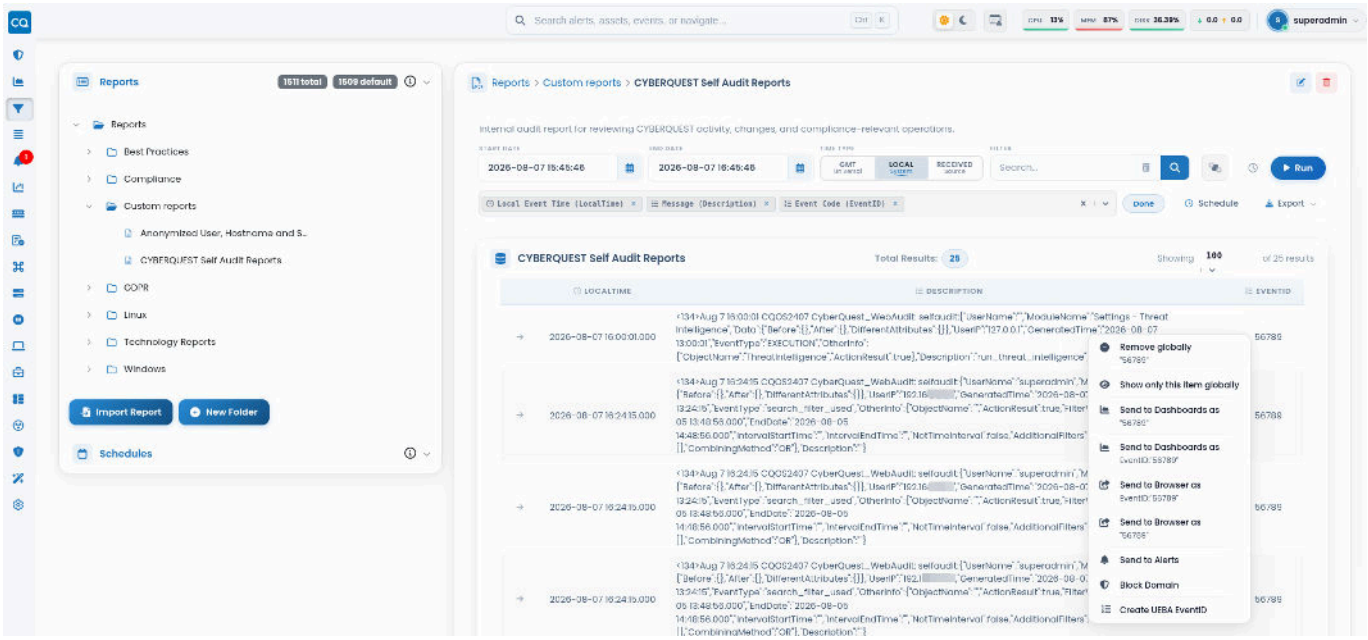


button to execute the report. Execution time depends on the query complexity, volume of data to be searched, and the number of items to be displayed. A simple search will list any volume in a matter of seconds.



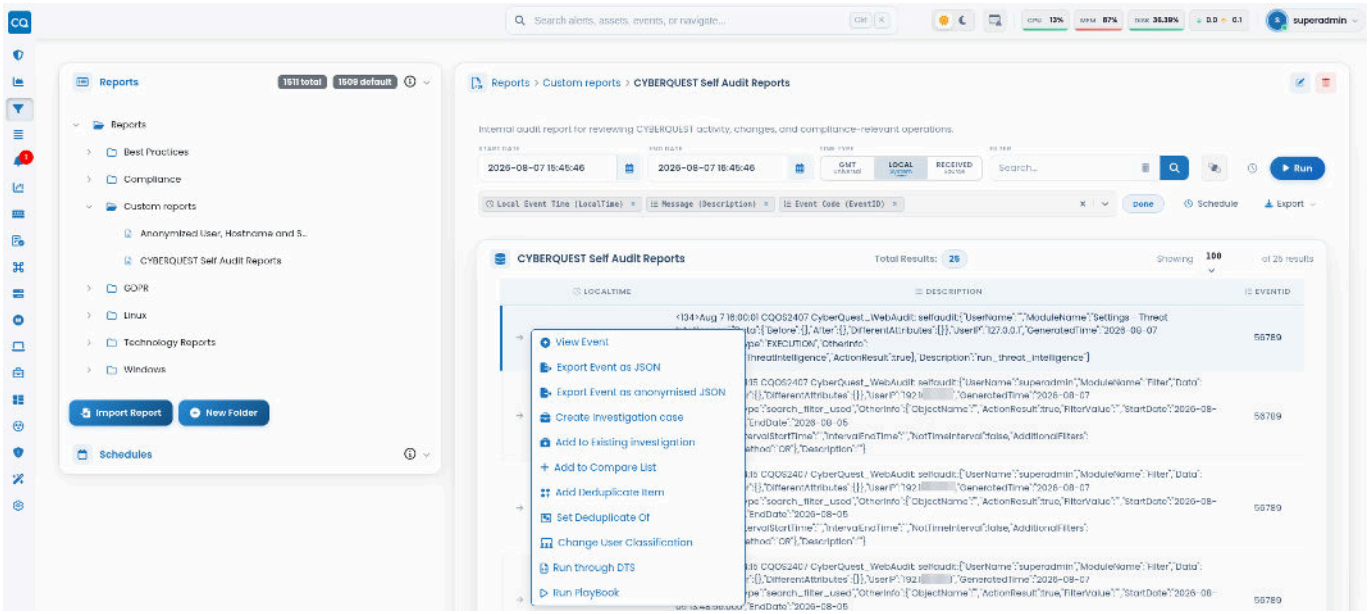
All report results are dynamic, enabling further actions to expand the scope of reporting.

Clicking on any report field (except **Description**) opens a persistent pop-up menu with the following options:



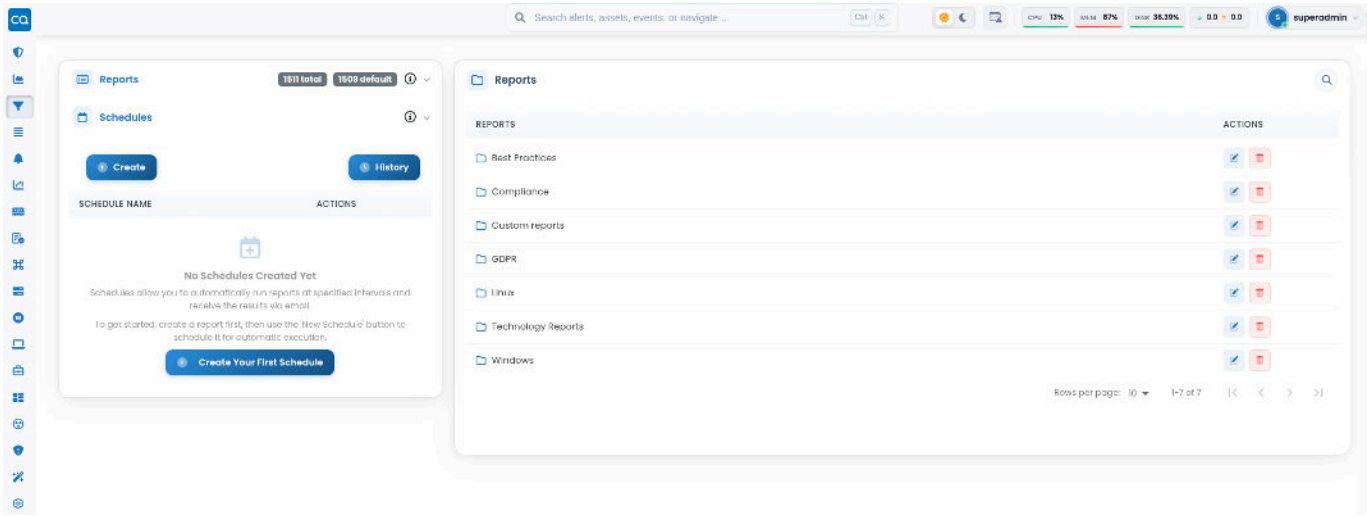
- **Remove globally:** Generates a search query that excludes all events containing the selected field value. The resulting query is applied in the **Search** box.
- **Show only this item globally:** Filters the report results to display only events that match the selected field value. The updated query appears in the **Search** box.
- **Send to Dashboards as `<value>` or `<field>`:** Opens the **Dashboards** module in a new browser tab and displays search results filtered by the selected value or field.
- **Send to Browser as `<value>` or `<field>`:** Opens a new **Browser** tab showing events filtered by the selected field or value.
- **Send to Alerts:** Opens the **Alerts** module in a new browser tab and uses the selected field value to create and display a corresponding alert configuration.
- **Block Domain**: Blocks the domain identified in the selected event, allowing the user to quickly restrict access to suspicious or potentially malicious domains directly from the report results.
- **Create UEBA EventID**: Creates a UEBA entry from the selected EventID, enabling the event type to be included in behavioral monitoring and anomaly analysis.

The event list view provides a wide range of actions for interacting with individual events. These options enhance analysis, investigation, and reporting capabilities directly from the event table.



Managing report schedules

Selecting the Schedules option in the Reports and Schedules section of the Reports module displays a list of all defined report schedules.



For any of the schedules listed here, you can edit and delete them. You can also create a new schedule by pressing **New Schedule** button.

Adding a new schedule or editing an existing one opens **Edit schedule** pop-up window described above.

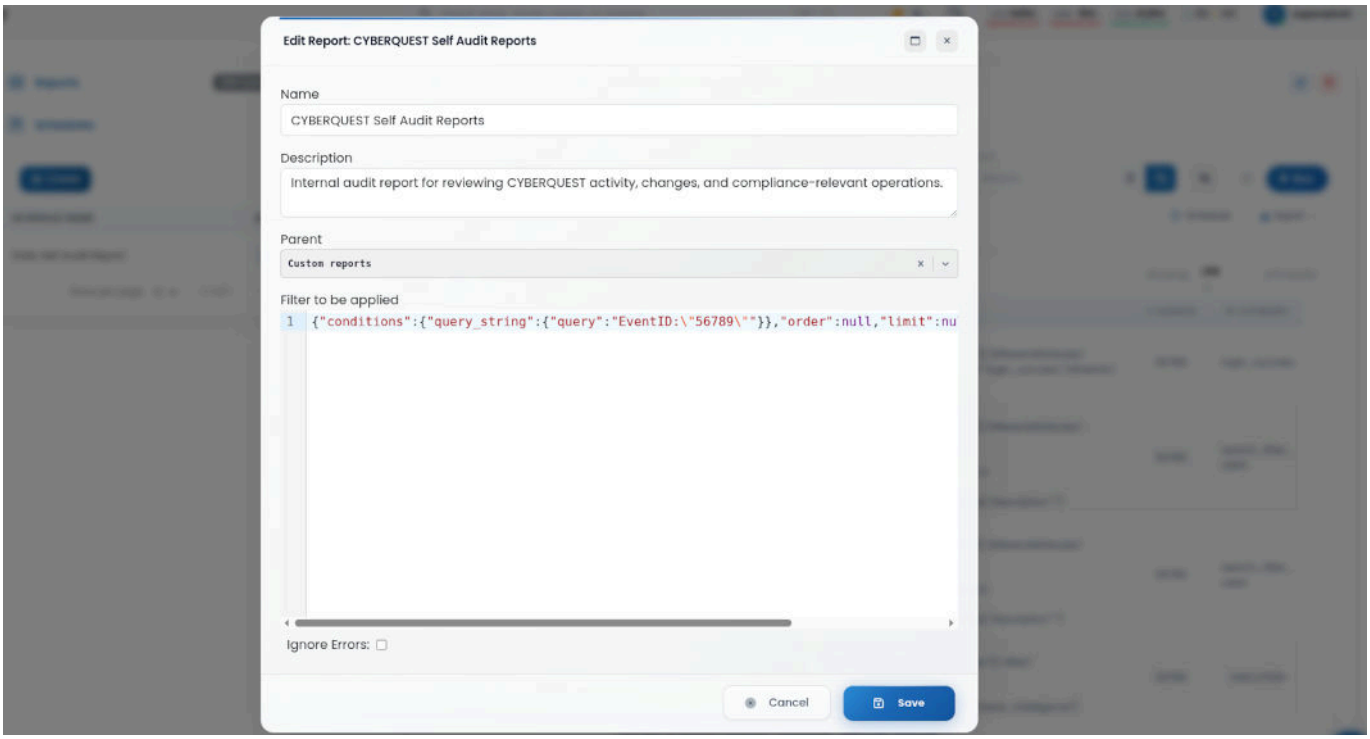
Editing reports

To edit a selected report, click the



button displayed next to the target report in the **Reports** list. This action opens the **Edit Report** pop-up window:

- **Name**: Modify the report name, or leave the existing name unchanged.
- **Parent**: Use the drop-down list to move the report to a different folder within the report structure.
- **Description**: Update the report description, or retain the current text.



Press “Save” to apply the changes, or “Cancel” to discard them and return to the main interface.

Deleting reports

To delete a selected report, click the



button displayed next to the target report in the Reports list.

A confirmation dialog will be displayed. Click ***Confirm*** to proceed with the deletion, or click ***Cancel*** to close the dialog and return to the main interface.

Export data from reports

The module supports both scheduled and ad hoc reporting all, at once or granularly providing a complete overview of compliance and operational activity within the IT environment.

For detailed instructions on how to export data from Reports, refer to: How to export data from Reports.

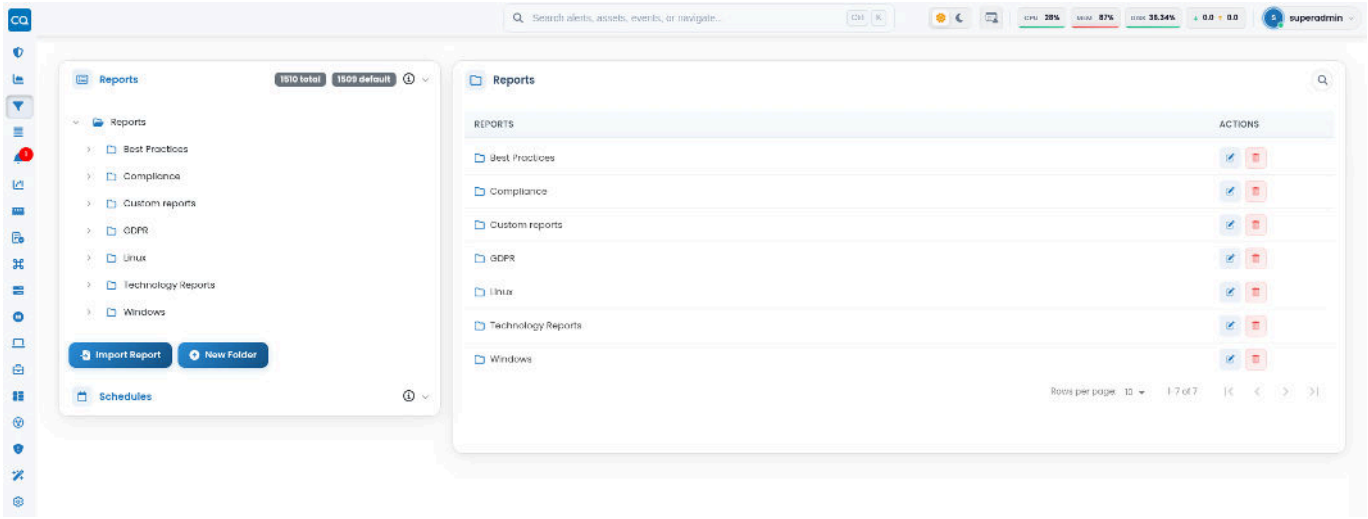
Import reports

A report definition can be imported from an external .CQO file, which uses CYBERQUEST’s proprietary format.

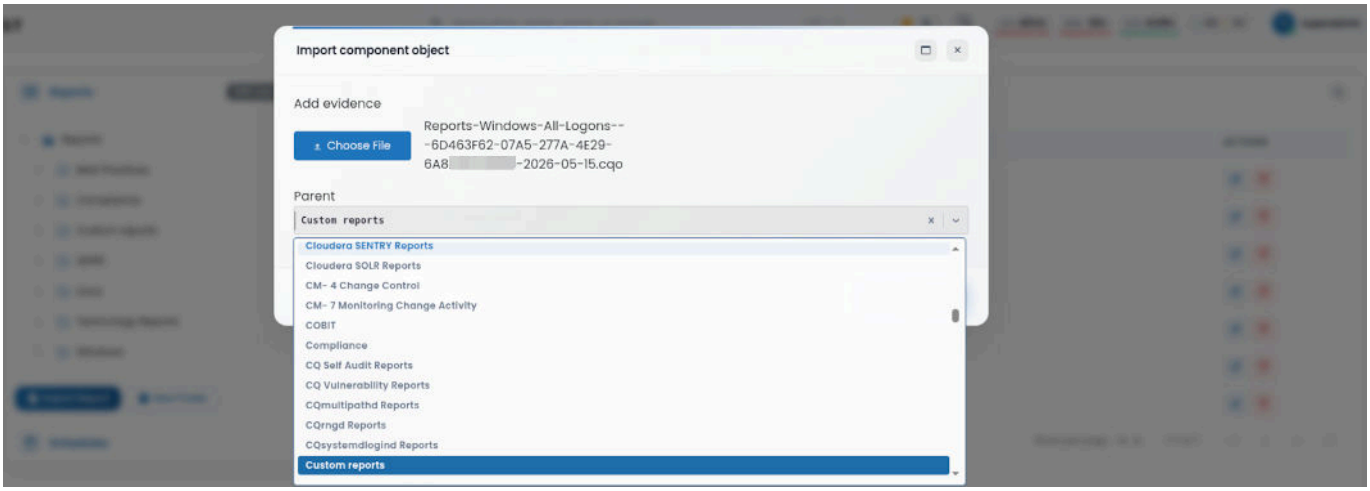
To import a report definition, click the



button.

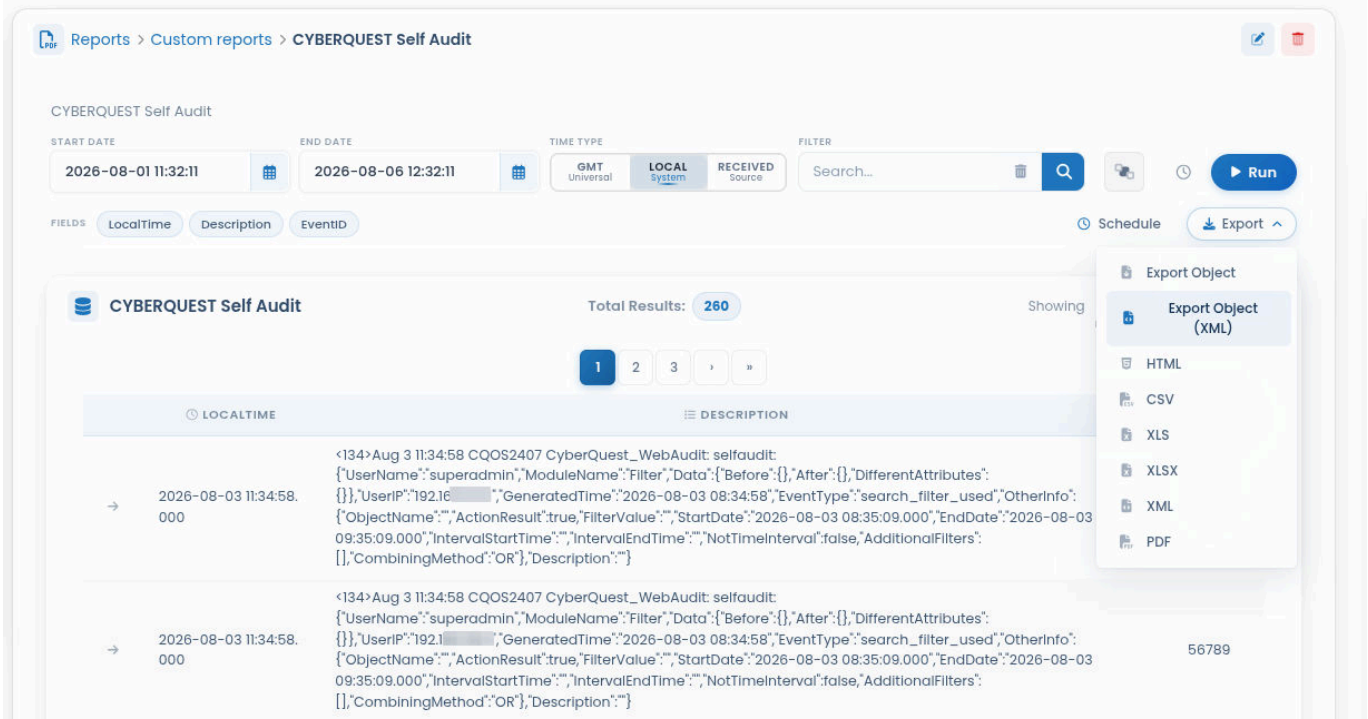


Next, select the file to be imported and specify the Parent folder - this defines the location where the report will be added.



Import and export report definitions

Report definitions can be imported and exported in XML format directly from the Reports module. Click **Import XML** to import an existing report definition. To export the selected report definition, open the **Export** menu and select **Export Object (XML)**.



This XML file does not appear to have any style information associated with it. The document tree is shown below.


```
<Reports>
  <name>CYBERQUEST Self Audit</name>
  <added>2026-08-06 09:32:05</added>
  <active>1</active>
  <parent_id>634</parent_id>
  <isFolder>0</isFolder>
  <isDeleted>0</isDeleted>
  <query>{"conditions":{"query_string":{"query":"EventID:56789"}},"order":null,"limit":null,"page":null,"sort":null,"aggs":null}</query>
  <params>{"selectedFields":"WyJMb2NhbFRpbWUiLCJEZXNjcmlwdGlvbiIsIkV2ZW50SUQiXQ=="}</params>
  <description>CYBERQUEST Self Audit</description>
  <guid>D297A194-5209-0BE1-3534-667DDCCDD84E</guid>
  <parent_guid>E98DA040-ADDC-19ED-092E-3A5A996C65B4</parent_guid>
  <security_score>10</security_score>
  <security_level>1</security_level>
  <extension_guid/>
  <version/>
  <ObjectName>CYBERQUEST Self Audit</ObjectName>
</Reports>
```


Note: Exporting a report definition is different from exporting the report results. The Export Object (XML) option exports the report configuration, while the other available formats export the data returned after running the report.

Report execution scenario example

Step 1: Open the **Reports** module from the Web Interface.

Step 2: Navigate to the **Windows** reports folder and select the **Windows All User Activities** report.

Step 3: Define the desired **Start Date** and **End Date** for the report.

Step 4: In the Filter Data field, enter simple or complex queries using logical operators (AND, OR, NOT). For example, to generate results for specific users and a particular category (e.g., Logoff), a filter like the following can be used:

```
UserName:(user1 OR user2) AND EventCategory:Logoff
```

Step 5: Search results are displayed in the lower section of the web page, sorted in ascending chronological order. To view event details, click on the corresponding field. The results section also shows the total number of results (**Total results**), the number of pages, and the currently active page.

How to create a new report and how to run it

For detailed instructions on creating and running a new report, refer to the following guide: How to create a new report and how to run it

Browser

Introduction to the Browser Module

The Browser module is designed to provide a detailed, real-time view of events collected by CYBERQUEST. It offers operators and analysts a flexible interface to examine logs, investigate anomalies, and validate filtering rules across a wide range of data sources.

Browser can be accessed at any time by clicking the



button located in the left-side navigation panel of the Web Interface.

Working with Browser module

The **Browser** module interface is organized into three main sections, each supporting a specific aspect of event analysis:

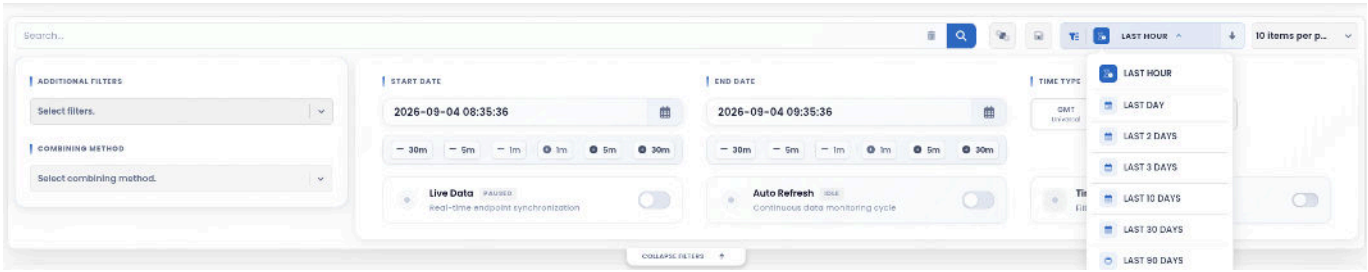
- **Search and Filter**: Enables granular control over the displayed information. This section allows the use of advanced search queries and filters to narrow down or expand the event data shown in the results.
- **Results**: Displays the list of events matching the defined criteria. This section presents the actionable data in tabular form, allowing sorting, detailed inspection, and redirection to other modules.
- **Geolocation**: Provides a graphical representation of events on a world map, based on originating or destination IP addresses. This visual aid supports the identification of geographic patterns or anomalies in the data.

Browser Search and Filter section

This section provides control over the information displayed in the **Browser** module. It allows the definition of additional filters and logical combinations for event data within a specified date and time range.

To access the **Search and Filter** section, expand the filters panel by pressing the

button. The panel will then be displayed:

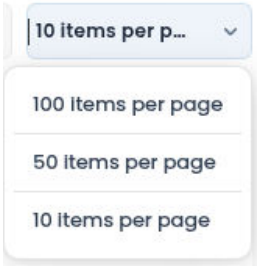


1. The **Search field** allows filtering of displayed data using free text queries. If left empty, all available events are shown.

A similar search capability is available in the **Dashboards** module. For detailed usage instructions, refer to the guide:Using Searches.

Unlike the **Dashboards** module, an additional drop-down list is available next to the **Search** field in the **Browser** module.

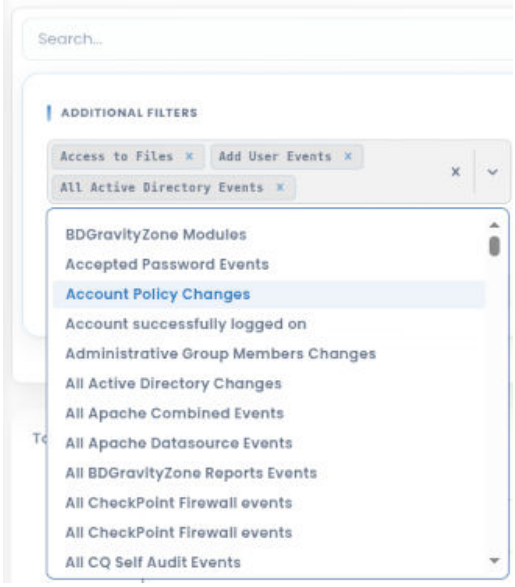
By clicking the

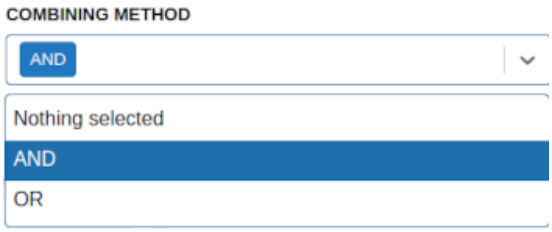


button, the number of displayed items per page can be adjusted. The default is 10, with options to increase to 50 or 100 items.

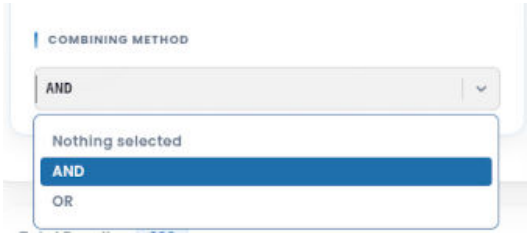
2. Additional filters can be applied using the **Filtering options** section. By default, no filters are selected. Opening the **Additional filters** drop-down list reveals a wide range of predefined filters organized by technology. One or multiple filters can be selected as needed.

The **Combining method** drop-down list is used to define how the selected filters are applied together. Available options include the **AND** and **OR** logical operators. The selected operator applies globally to all chosen filters.





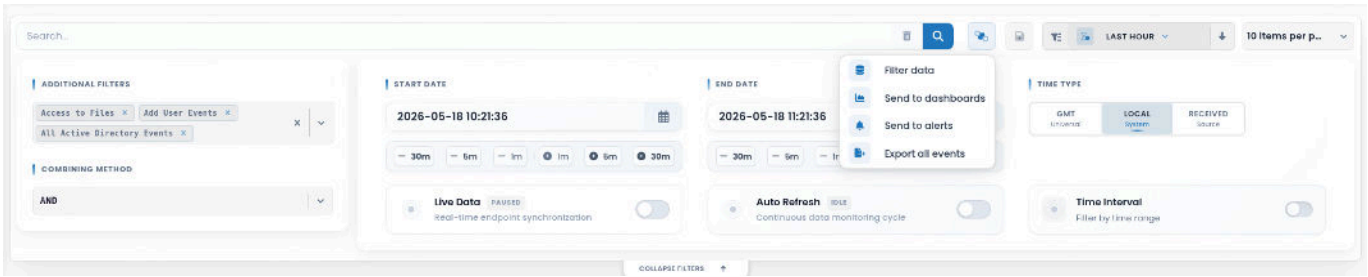
After completing the selections, navigate to **Query Actions > Filter** to apply the chosen filters



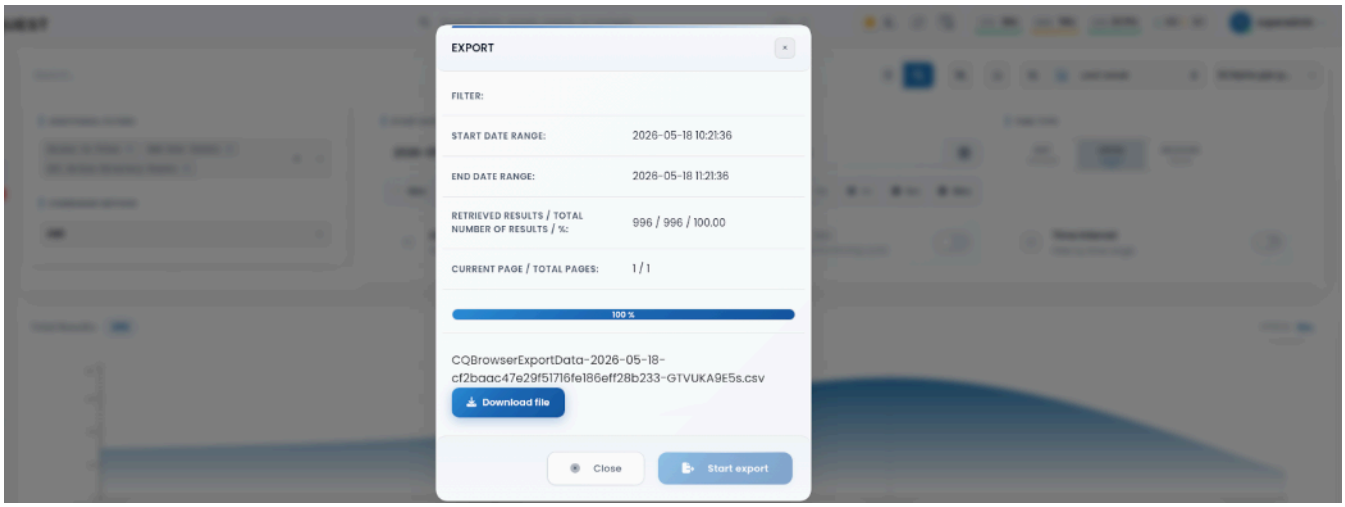
Additional options available in the Search and Filter section:

To view this section, expand the filter panel by pressing the

button. The filter options will then be displayed:



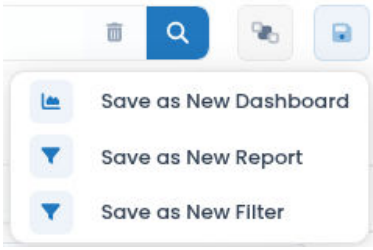
- **Send to Dashboards**: Opens the **Dashboards** module in a new browser tab, displaying the filtered results based on the current selection.
- **Send to Alerts**: Opens the **Alerts** module in a new browser tab, listing the filtered results accordingly.
- **Export All Events**: Generates a CSV file containing all events displayed in the **Results** section. Due to the potential volume of data, this may take time. A status window will display the export progress percentage. Once the process reaches 100%, the file can be saved by clicking the **Download report CSV** link.



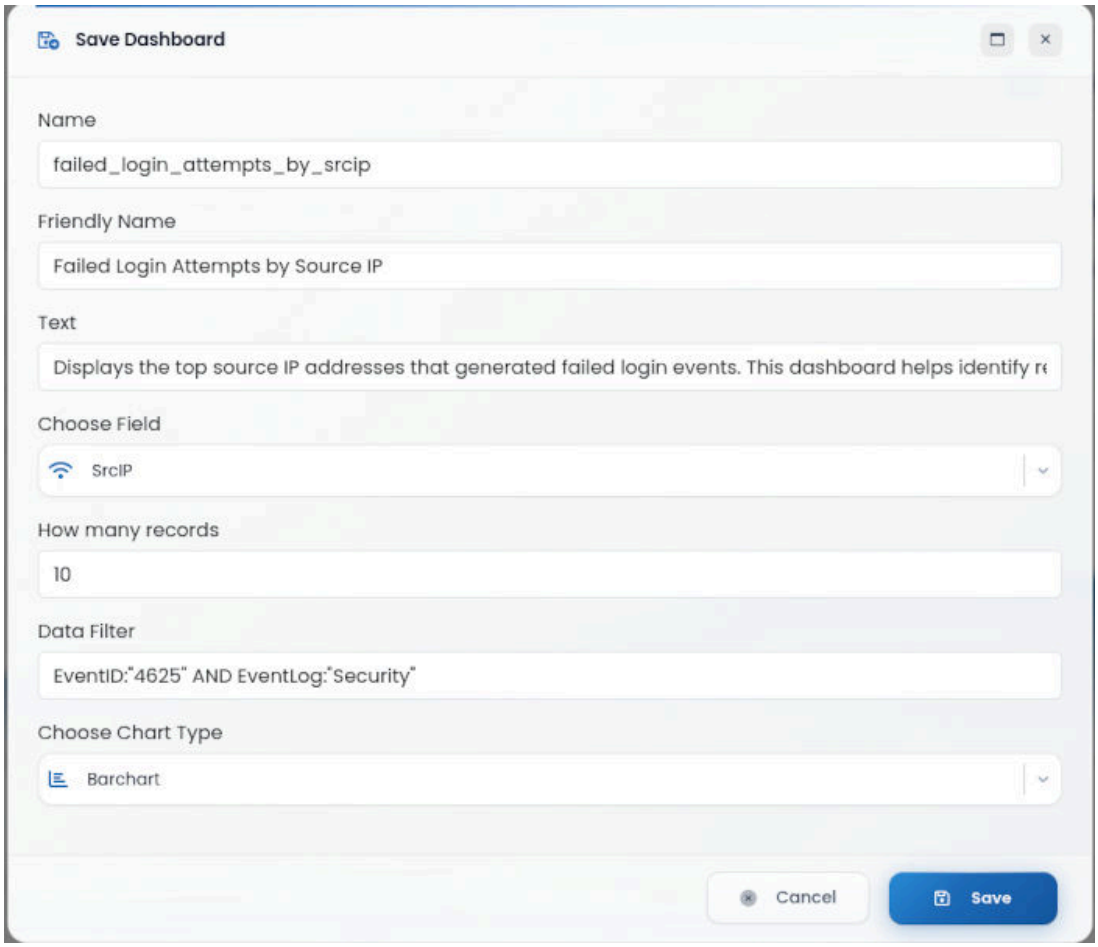
The current filter selection can be saved at any time. Pressing the



button opens three options for saving the filter configuration permanently:



- Save as **New Dashboard** opens the **Save as New Dashboard** window, allowing the creation of a new dashboard. The following parameters must be configured:
  - A convention-based name for the dashboard, which will appear in dashboard lists
  - A descriptive, user-friendly name, displayed in the Dashboards interface
  - A description outlining the type of information presented in the dashboard
  - The field used for graph generation
  - How many records to display in the chart
  - A Data Filter that defines the search conditions to be applied for generating the dashboard content
  - Graphic type (barchart, pie, gauge etc.)

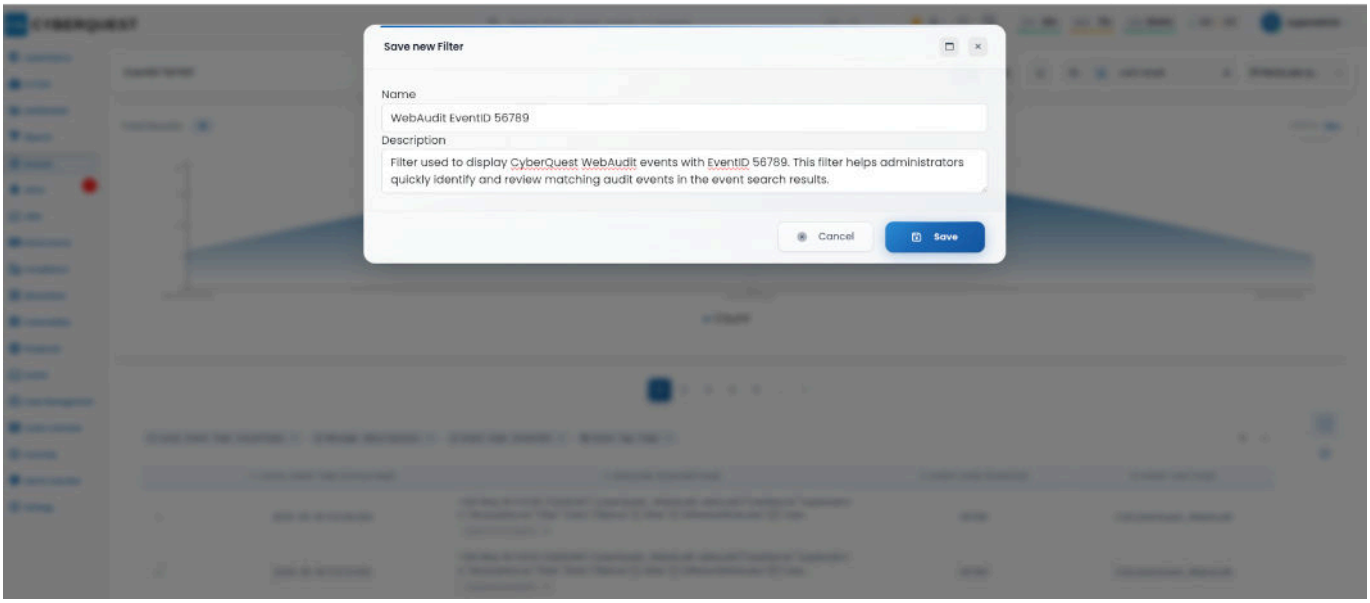


- **The Save as New Report** option opens the **Save as New Report** window, allowing the creation of a new report based on the current filtered data. To save a new report, a **Data Filter must be configured first**. If no filter is applied, the report cannot be saved. A report name and description must also be provided before saving the configuration.
- The **Save as New Filter** option opens the *Save as New Filter* window, enabling the creation of a new filter based on the criteria currently defined in the Search area.

  Note: This option can be used only after a filter condition has been defined in Search. If no filter criteria are configured, the filter cannot be saved.

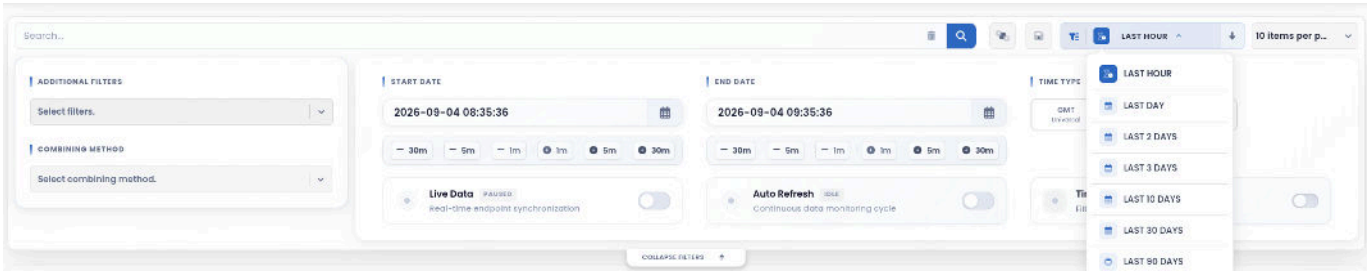
  A filter name and description must be specified before saving the configuration. The following parameters must be configured:

  - **Name**: The unique identifier for the filter, displayed in ***Settings > Management > Filters***. It is used to reference and manage the filter.
  - **Description**: Provides additional context about the filter's purpose and criteria, helping administrators understand what events or conditions the filter applies to.



3. The **Search and Filter** section includes options for **setting the date and time interval** to define the time range of the displayed information. This feature provides a quick overview of compliance data over a specified period.

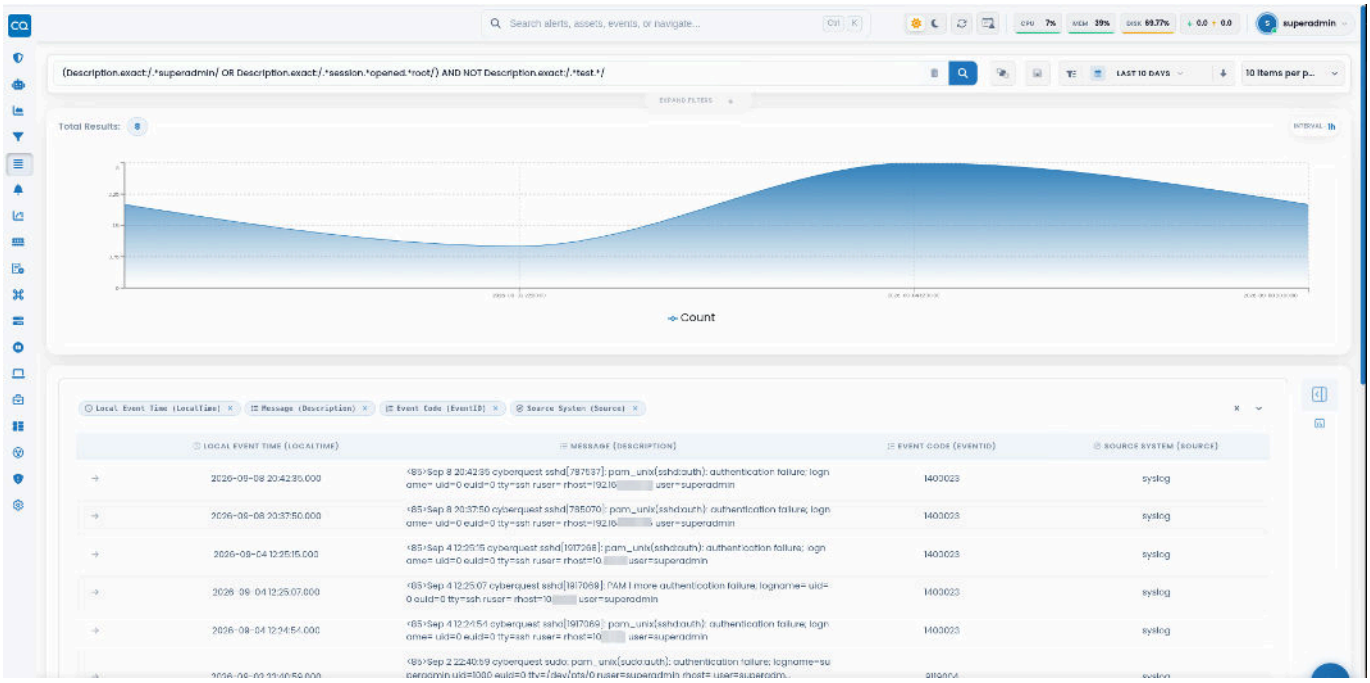
The interface provides options to define a specific start and end date, along with predefined date ranges (e.g., last hour, last day, last two days, last three days, last ten days, last 30 days, last 90 days). By default, the Dashboards interface displays data from the last hour. Additional controls beneath the **Start Date** and **End Date** fields allow for quick adjustment of the time interval and selection of the time reference to be used, including GMT, Local Time, ReceivedTime, Now, AutoRefresh, TimeInterval, and Not in this time interval.



- **GMT** - is the time reference which converts your search time into GMT (Greenwich Mean Time Zone).
- **LocalTime** - is the time reference when an event occurred.
- **ReceivedTime** - is the time reference when the events arrived in CYBERQUEST machine.
- **Now** - self-update end data with current time.
- **Live Data** - Keeps the time range synchronized with the current time, continuously updating the displayed date/time window without automatically refreshing the event results
- **AutoRefresh** - Periodically refreshes the results using the current time window, displaying the latest events according to the configured refresh interval
- **Time Interval** - the search is made from Start Time to End Time interval
- **Not in this time interval** - the search outputs the events that are NOT between Start Time and End Time

Regular expression searches

Example of a regular expression (RegEx) query in CYBERQUEST Browser. RegEx patterns can be combined with Boolean operators such as AND, OR and NOT to filter events based on field values. For text fields exposing an exact/non-analyzed representation, the `.exact` field can be used when applying RegEx patterns.

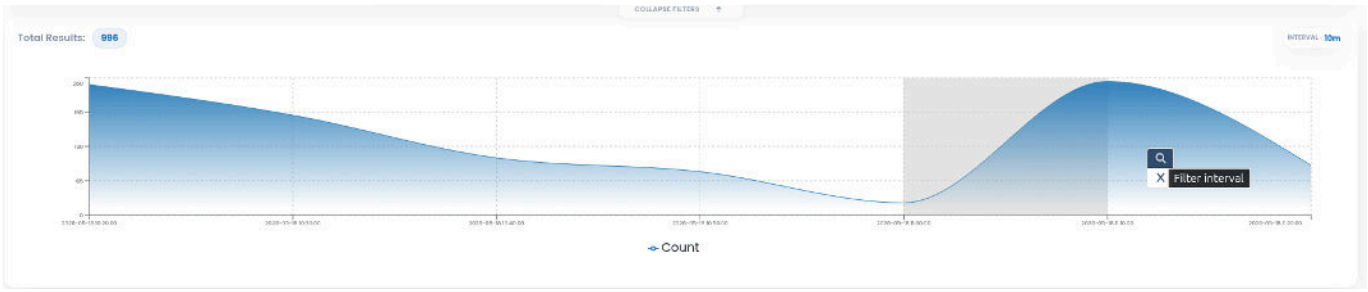


Events overview graphic

This chart from the Browser module displays the total number of events in samples within the selected time interval.



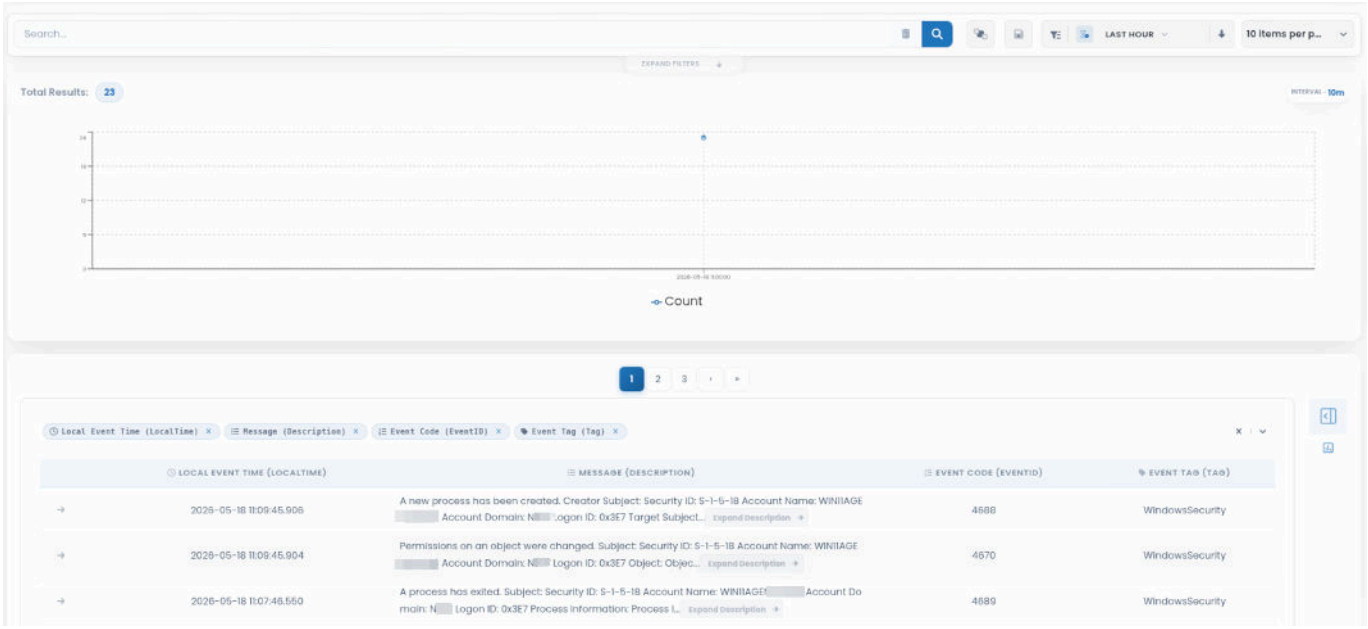
To filter events within a specific time interval, click and drag across the graph to highlight the desired time range. The displayed events will adjust to match the selected interval.



After selecting the time range, click the Filter interval

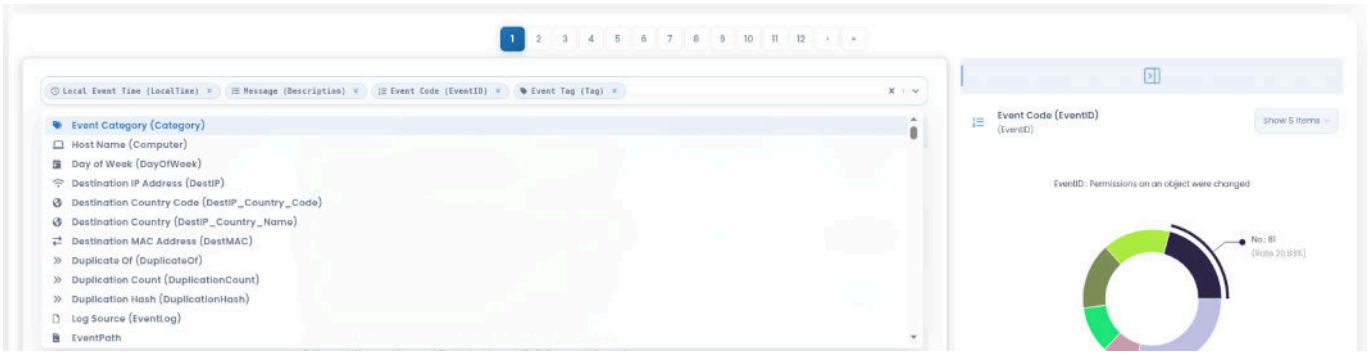


button. The **Browser** module will then display all events corresponding to the selected time interval.



Results section

This is the main display area for browsing activities. All events are listed in chronological order, the number of items on a page being the one set in **Search and Filter** options.



Not all event fields are shown by default. Fields can be customized by clicking

in the field selection bar, which opens a drop-down list of available fields. Fields can be added by selecting them from the list and removed at any time by clicking the **x** next to a selected field. The following fields are available to add:

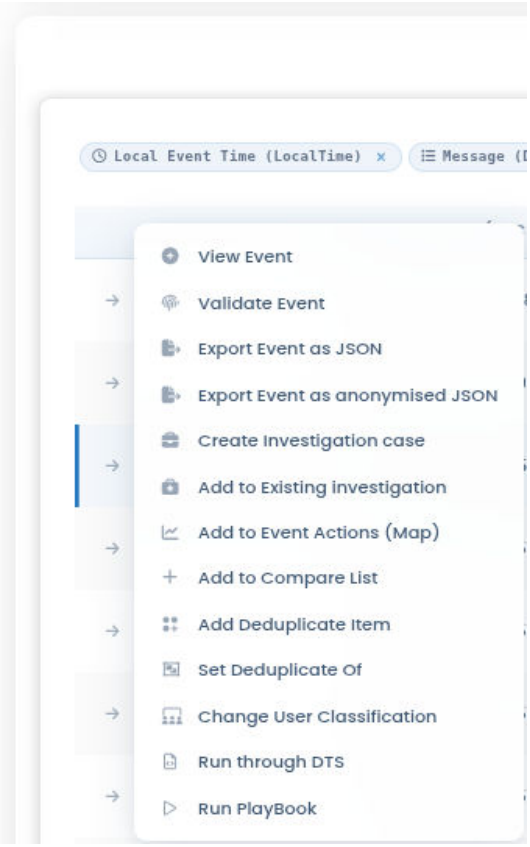
To see more information about the Log Record Fields, please follow the link: Log Records structure.

Anonymized fields Depending on the permissions assigned to the user's group, anonymized event fields are displayed either in anonymized form or with their original values. See **Decrypt permission** in the Groups configuration section for details.

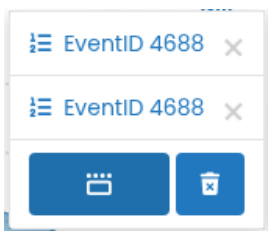
Browser interface allows users to interact with the listed events. For each event, clicking the



icon on the left opens a drop-down menu with the following options:



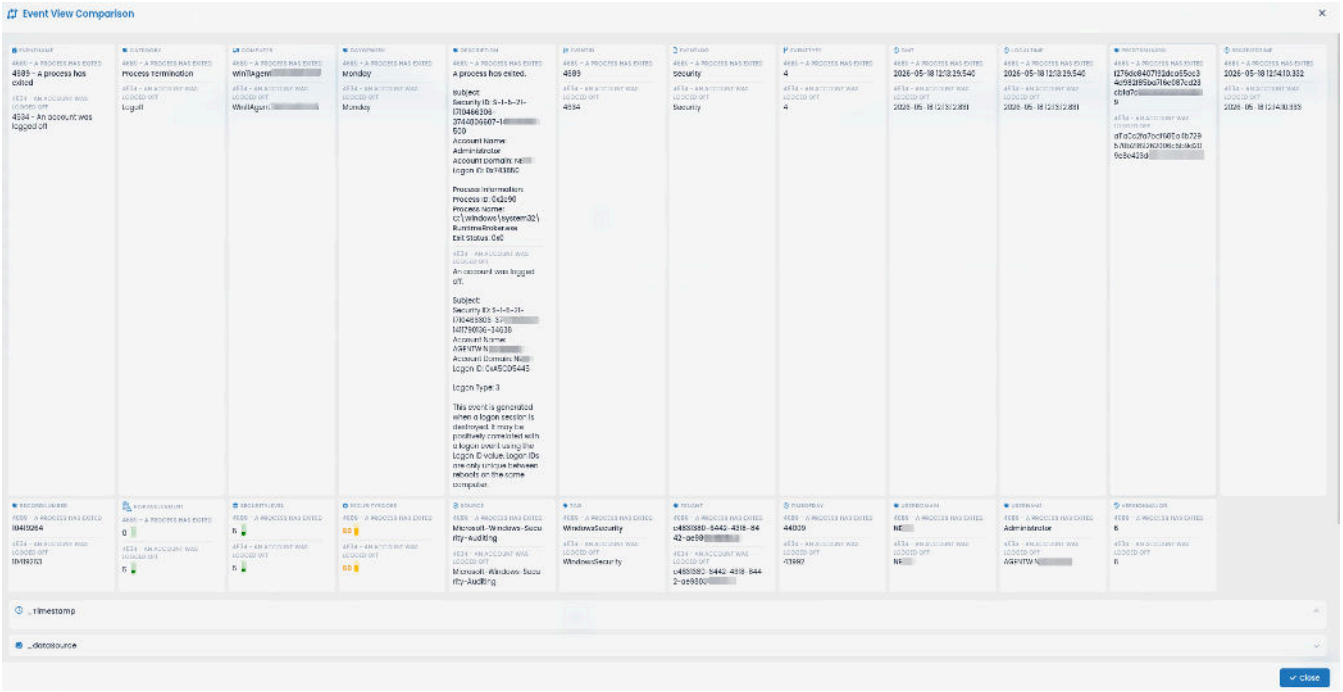
- **View Event** - Opens a detailed information window displaying all data fields associated with the selected event.
- **Validate Event** - Verifies the cryptographic integrity of the selected event. The action opens the Validate Event Hash panel, displaying the SHA-256 hash associated with the event and allowing the RawData payload in Base64 format to be validated against the stored hash.
- **Export Event as JSON** - Exports the full event data in JSON format for external analysis or archival purposes.
- **Export Event as anonymised JSON** - Exports the event in JSON format with sensitive or identifying information anonymized.
- **Create Investigation case** - Opens the **Add Evidence to New Case** window, allowing users to initiate a new investigation based on the selected event. See *CQ 2.30 User Guide - Case Management Module* for more.
- **Add to Existing investigation** - Opens a selection window to attach the event to an already existing investigation case.
- **Add to Event Actions (Map)**- If the event contains a public IP with a known geolocation, it will be plotted on the world map in the **Geolocation** section for visual context.
- **Add to Compare List** - Adds the event to a comparison list, enabling side-by-side review with up to five events simultaneously.



After adding the events, click the

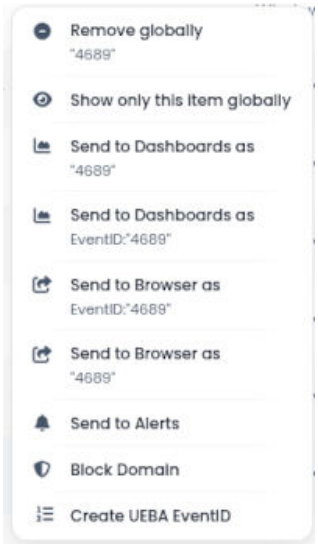


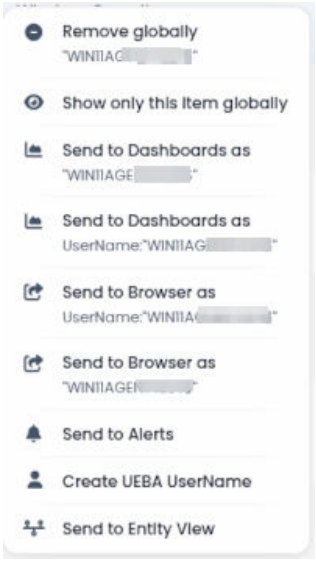
button located on the right side of the web interface to open the *Event View Comparison* window.



- **Add Deduplicate Item** - Marks the event as a potential duplicate to be used as a reference when identifying duplicate events.
- **Set Deduplicate Of** - Links the current event as a duplicate of a previously identified reference event.
- **Change User Classification** - Allows manual adjustment of the user classification assigned to the event (e.g., internal, external, trusted).
- **Run through DTS** - Opens the DTS testing window for the selected event, allowing the user to execute an active DTS object and compare the original event with the processed result.
- **Run PlayBook** - Executes a predefined PlayBook (automated response workflow) associated with the event's characteristics.

All fields, except **Description**, support contextual interactions within the **Browser** and other modules. Clicking on any field value of a specific event opens a drop-down menu with the following quick action options:





- **Remove globally**: Excludes all events containing the selected field value from the event list. The exclusion filter is automatically written in the **Search** box.
- **Show only this item globally**: Filters the event list to display only events containing the selected field value. The filter is automatically applied in the **Search** box.
- **Send to Dashboards as :** Redirects to the **Dashboards** module and applies the selected **field value** as a search query. Opens in a new browser tab.
- **Send to Dashboards as :""**: Redirects to the **Dashboards** module using a structured **field-value filter** (e.g., `EventID:"<Value>"`). Opens in a new browser tab showing only the matching results.
- Send to Browser as `<Value>`: Opens a new **Browser** tab and filters events using the selected **raw value** as a free-text search query, without specifying a field.
- **Send to Browser as :""**: Opens a new **Browser** tab and filters events using a **structured field-value** query (e.g., `EventID:"<Value>"`), displaying only the matching results.
- **Send to Alerts:** Redirects to the **Alerts** module, showing events that match the selected value. Opens in a new browser tab.
- **Block Domain**: Blocks the domain identified in the selected event, allowing users to quickly restrict access to suspicious or potentially malicious domains directly from the **Browser** interface.
- **Create UEBA EventID**: Triggers the creation of a UEBA (User and Entity Behavior Analytics) event using the selected field. This integrates the event into behavioral analysis workflows for anomaly detection and user/entity profiling. *Available only for fields like* `EventID`, `Computer`, *and* `UserName`.
- **Create Entity View:** Opens a contextual entity view based on the selected field, consolidating related activity and behavioral patterns to enhance investigation insights. *Available only for fields like* `EventID`, `Computer`, *and* `UserName`.

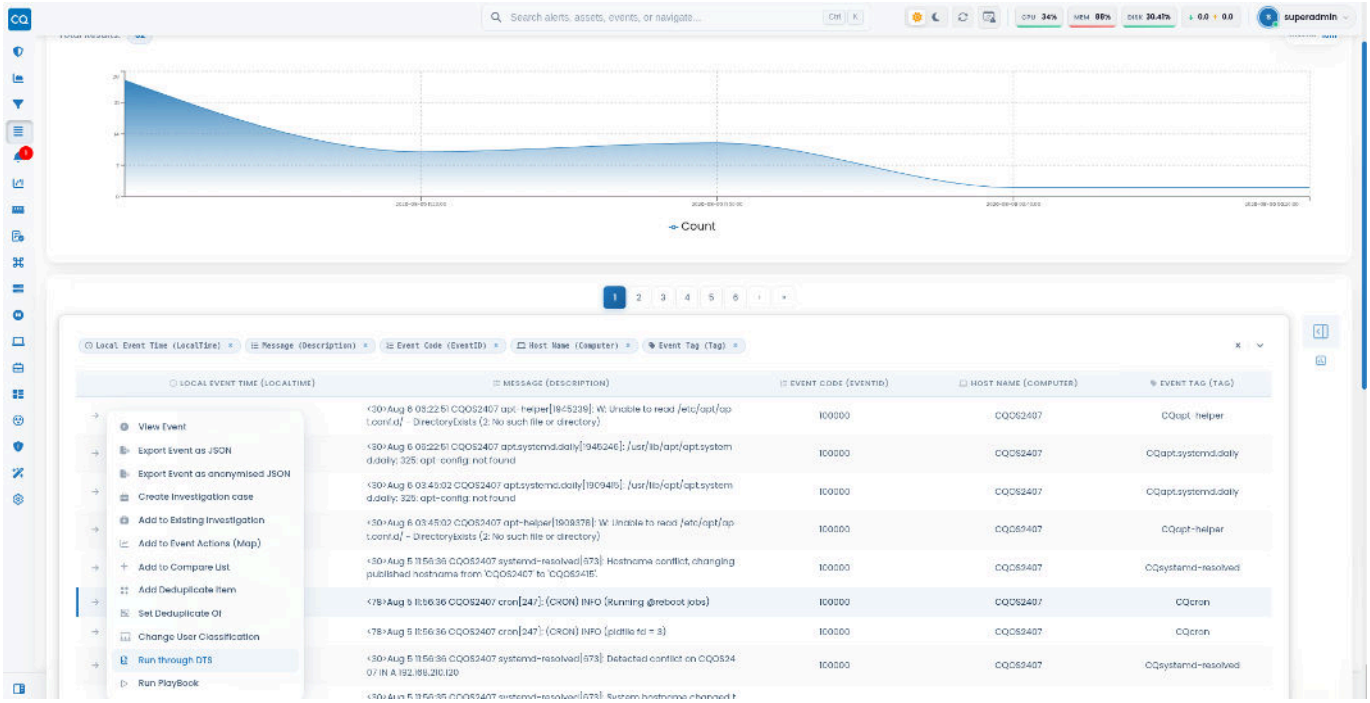
All the quick actions mentioned above work by generating search queries, which are automatically entered into the Search box. When multiple actions are applied consecutively without clearing previous ones, the Browser inserts an AND operator between the search terms to combine them. For example, applying two **Remove globally** actions results in a search query like:

```
NOT DestIP:"IP_Address_1" AND NOT Computer:"IP_Address_2"
```

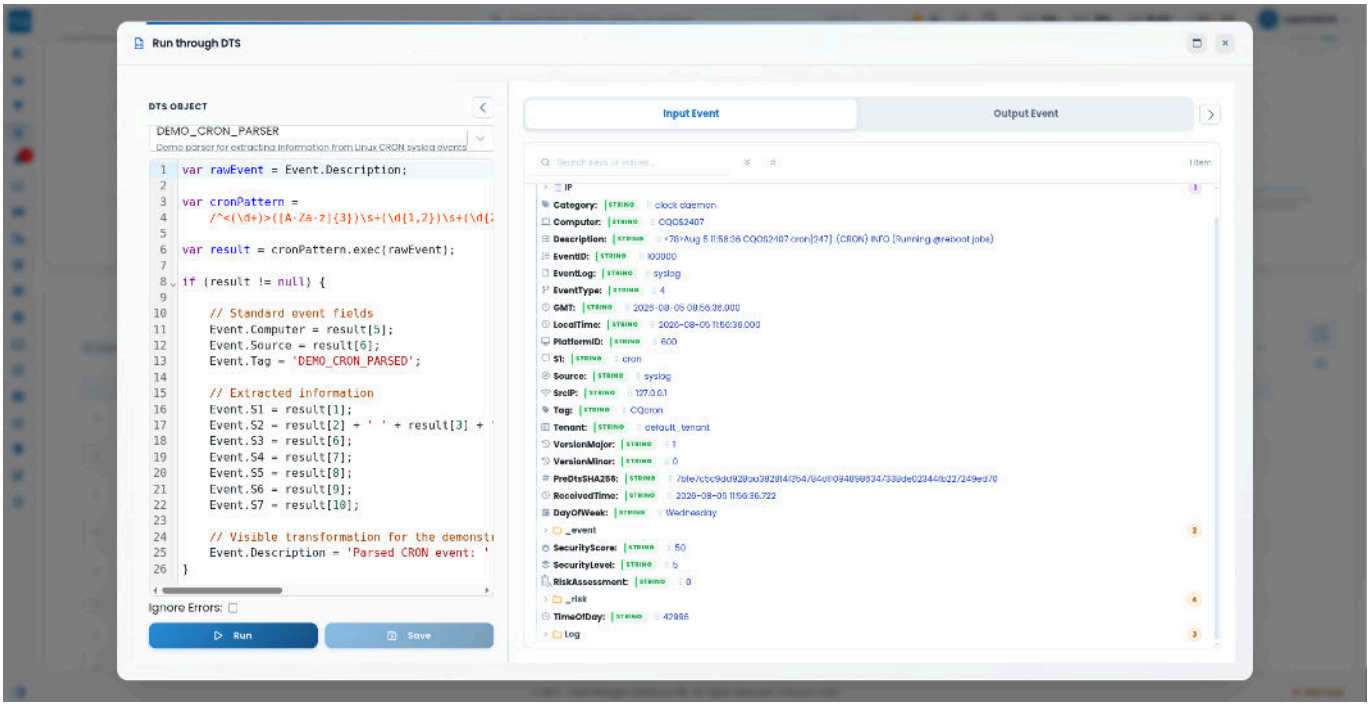
For further details, refer to *CQ 2.30 User's Guide, Using Searches*.

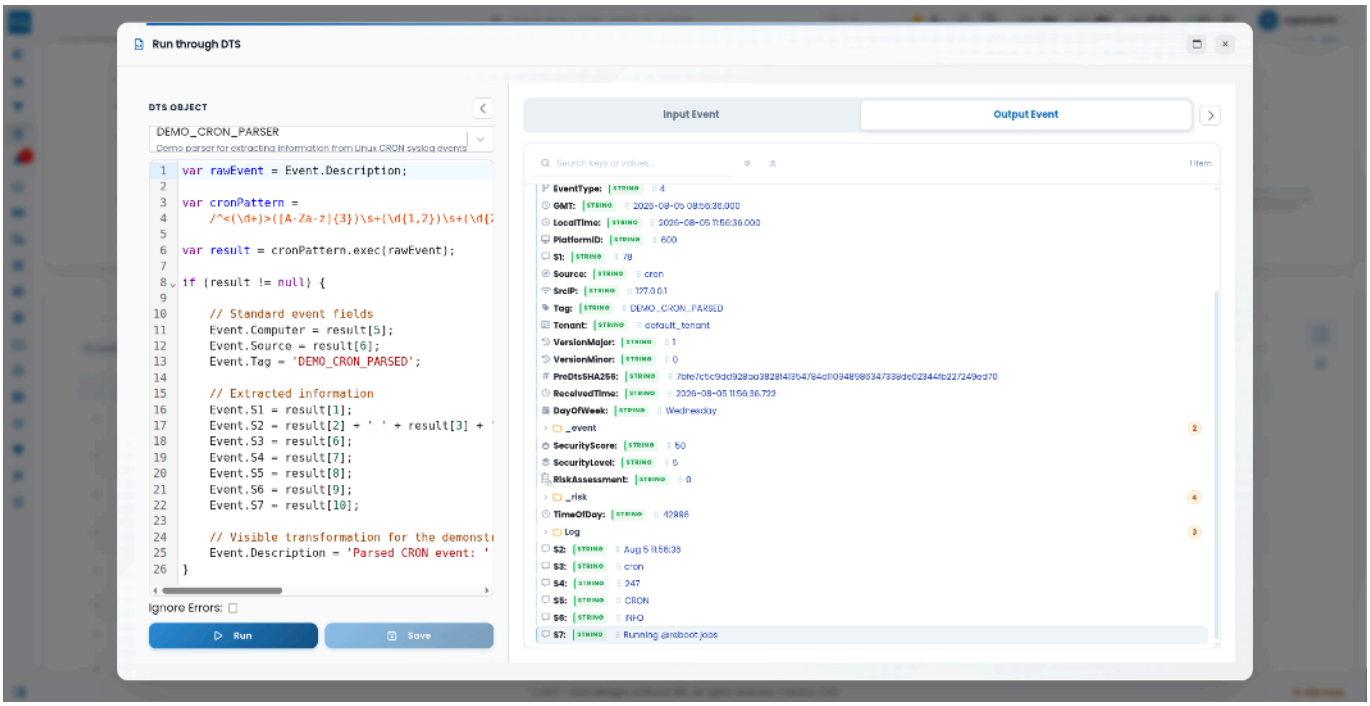
Testing a DTS parser from the Browser

CYBERQUEST allows DTS parsers to be tested directly from the graphical interface. Select an event from the Browser, open the event actions menu and choose **Run through DTS**.



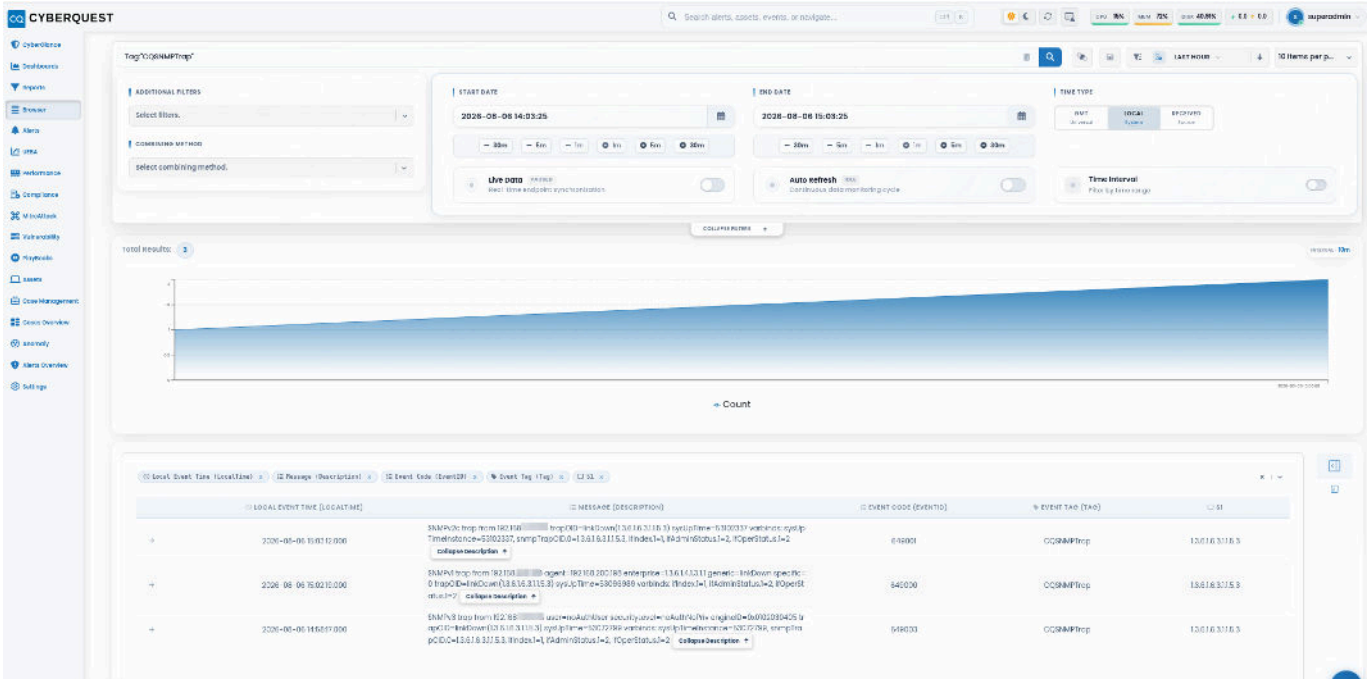
Select an active DTS object and press **Run**. The **Input Event** section displays the original event, while the **Output Event** section displays the event after processing.



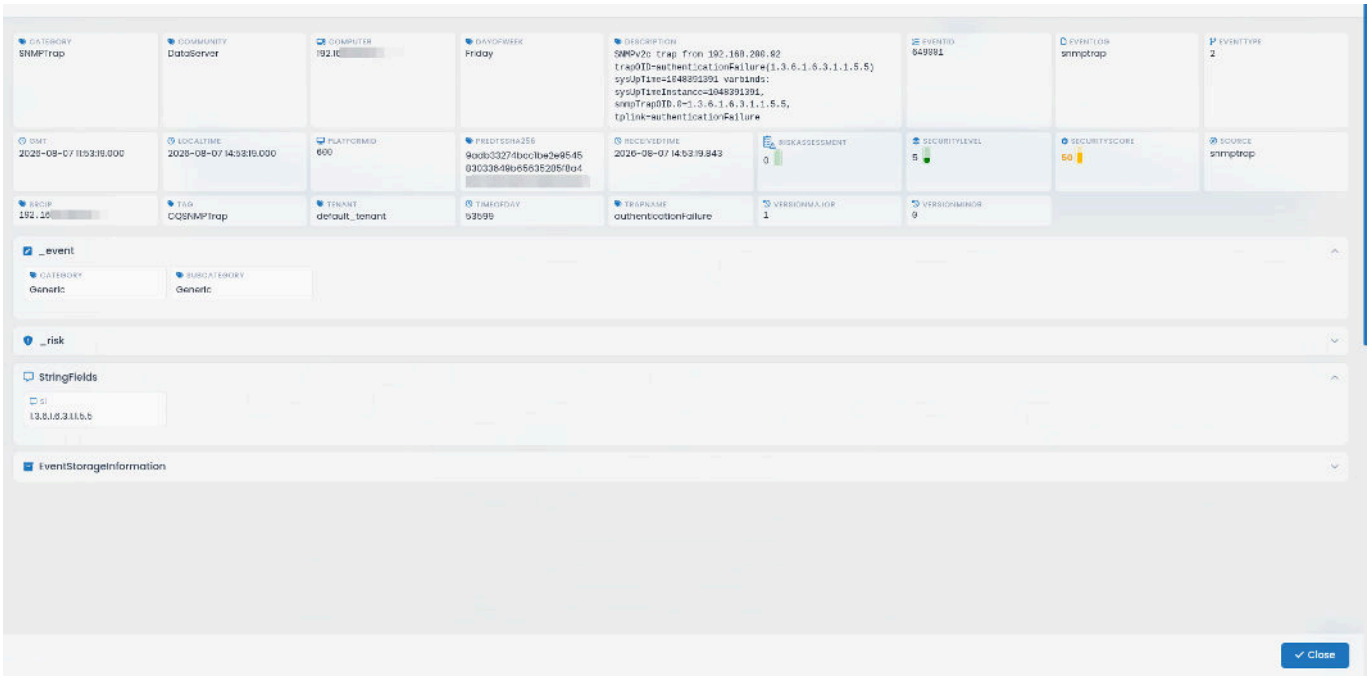


Viewing SNMP Trap events

SNMP Trap messages received by the CYBERQUEST Data Server are processed and made available as events in the Browser module. CYBERQUEST supports SNMPv1, SNMPv2c and SNMPv3 Trap events.



The detailed event view provides the parsed information associated with the received Trap, including the source address, EventID, event type, Trap OID, Trap name, timestamp and event tag.



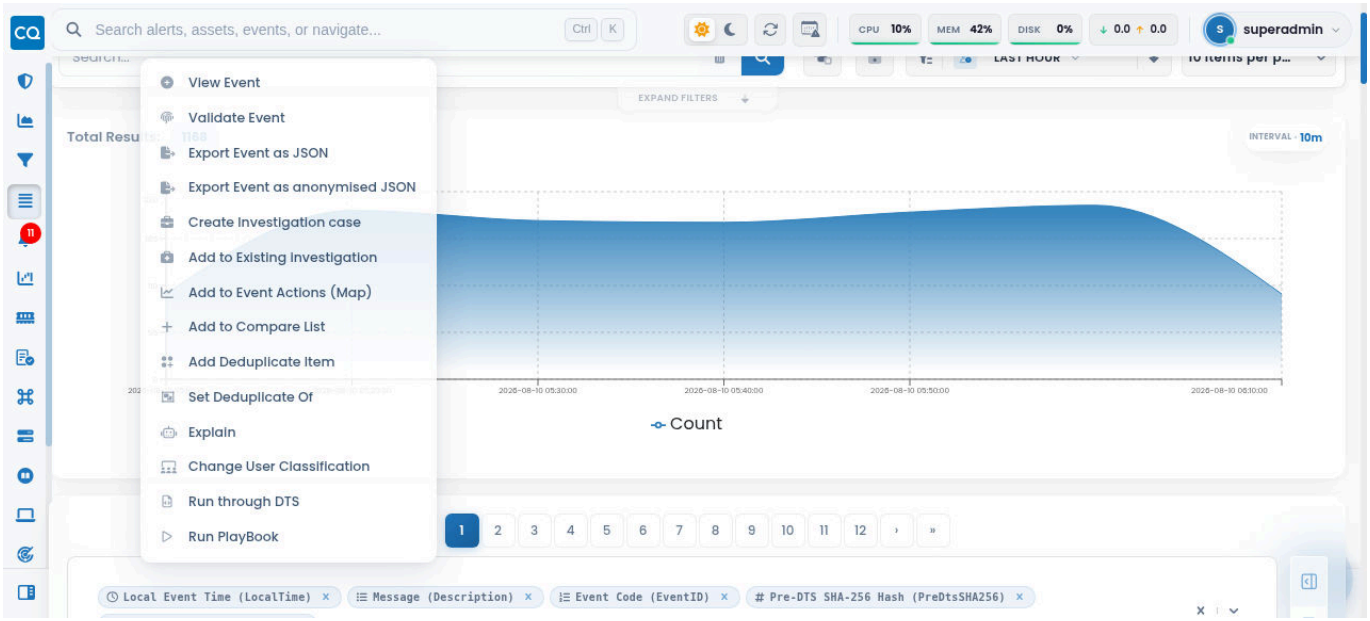
Verifying event integrity

Every event collected by CYBERQUEST is fingerprinted when it is stored. The Data Acquisition component computes a **SHA-256** hash over the raw event content, exactly as it was received from the source and before any normalisation, and saves it on the record in the **PreDtsSHA256** field. The raw content itself is kept alongside it in the **RawData** field.

The **Validate Event** action re-checks that fingerprint at any later point, so a stored event can be proven unchanged since the moment it was collected.

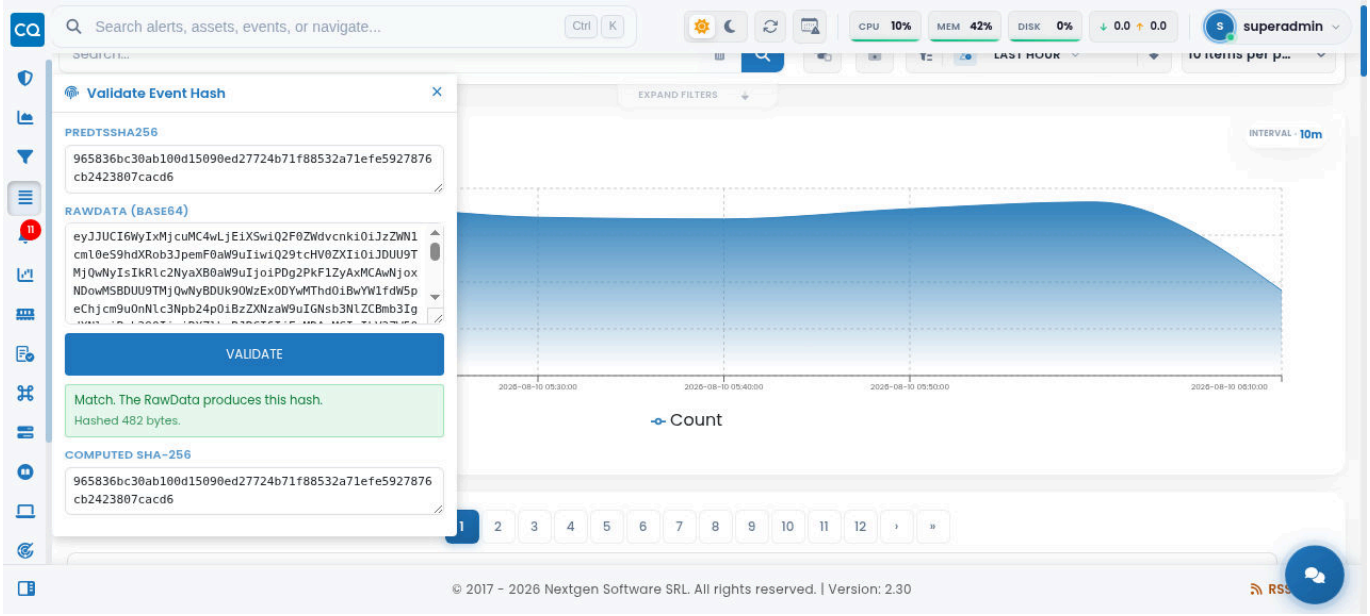
Running a validation

Select an event in the **Results** section, open the event actions menu and choose **Validate Event**.

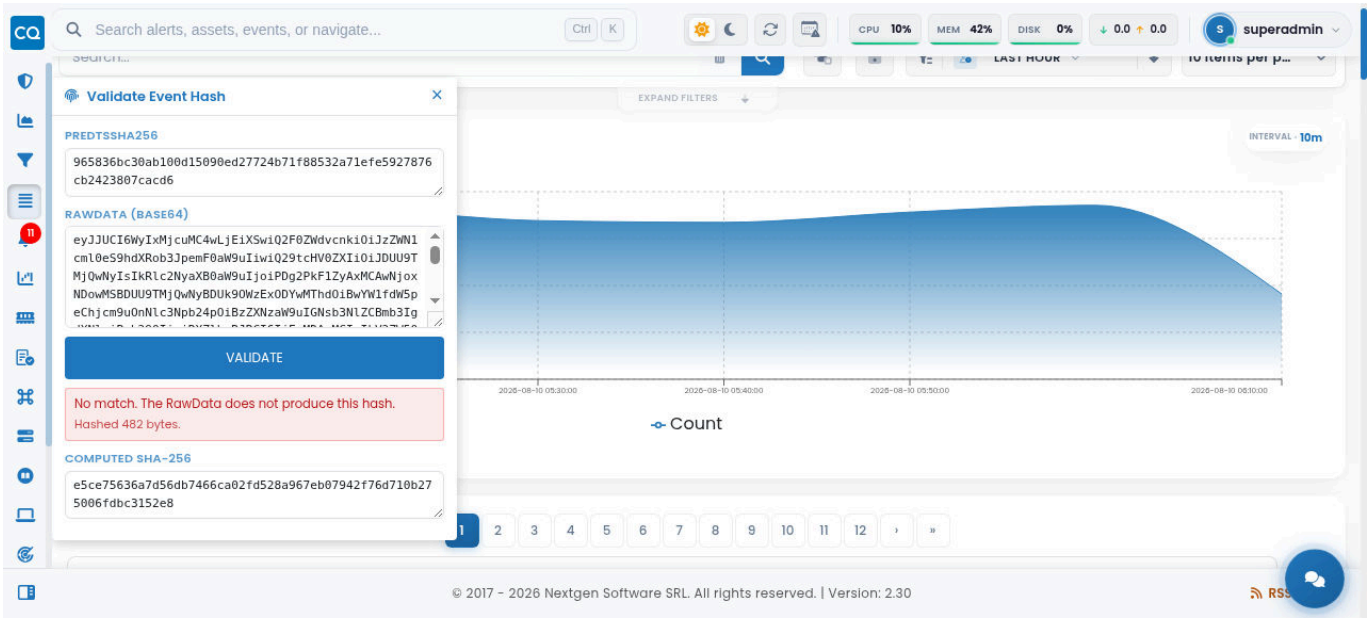


The **Validate Event Hash** panel opens with both values already loaded from the event, and the check already performed. The platform reads the stored **PreDtsSHA256**, reads the stored **RawData**, recomputes the SHA-256 hash over that content, and compares the result against the stored fingerprint.

When the two match, the event is intact. The panel confirms the result and reports how many bytes were hashed, together with the recomputed digest:



When the content no longer produces the stored fingerprint, the check fails and the panel says so. The example below is the same event after a **single byte** of its content was altered — the recomputed digest is completely different from the one stored at collection time:



Validating against an external copy

The panel also accepts values typed or pasted in by hand, which allows an event to be checked against a copy held outside the platform — an archive, an export, or the original source system.

To support that, both values can be copied straight out of the **Results** table. Add the **Pre-DTS SHA-256 Hash** and **Raw Event Data** columns through the field picker, and a copy button appears in each of those cells. The values are read back from the server rather than from the rendered table, so what reaches the clipboard is exactly what is stored, not a shortened display version.

RawData is copied **base64-encoded**. This keeps the payload intact as it travels through the clipboard and any text editor — line-ending conversion or stray whitespace cannot alter it and produce a false mismatch. The **RawData (base64)** field in the panel expects that same encoding.

Because both inputs are available in full, the verification can also be reproduced outside CYBERQUEST: decode the base64 payload and hash it with any standard tool, for example `sha256sum` or `openssl dgst -sha256`, and the result will match the value stored in **PreDtsSHA256**.

Note: Some data sources are configured to suppress raw event storage. On those events **RawData** is empty, so there is nothing to re-hash and the panel reports that the payload must be supplied manually. The stored **PreDtsSHA256** remains available and can still be checked against a copy of the payload kept elsewhere.

Events Manual Deduplication

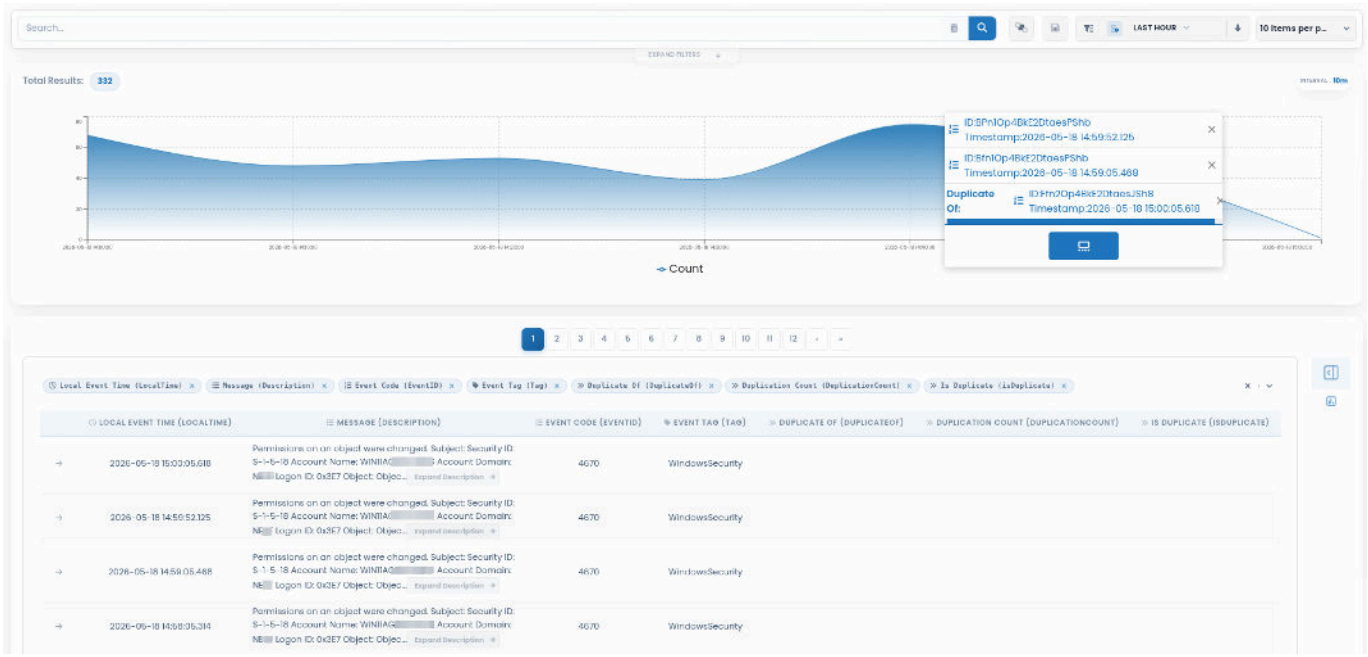
The **Manual Deduplication** functionality allows users to manually group similar or related events and mark one or more events as duplicates of a selected reference event.

This is useful when events are not automatically detected as duplicates, but the analyst determines that they refer to the same activity, incident, or repeated occurrence.

To manually deduplicate events, click the



button from the selected event row and choose one of the available deduplication actions:



Available Actions:

- **Add Deduplicate Item** - Adds the selected event to the deduplication list.

  This event can later be used as the reference event for other duplicate events.

- **Set Deduplicate Of** - Marks the selected event as a duplicate of one or more items previously added to the deduplication list using **Add Deduplicate Item**.

Manual Deduplication Workflow

1. Select the event that should be used as the reference event.
2. Click the

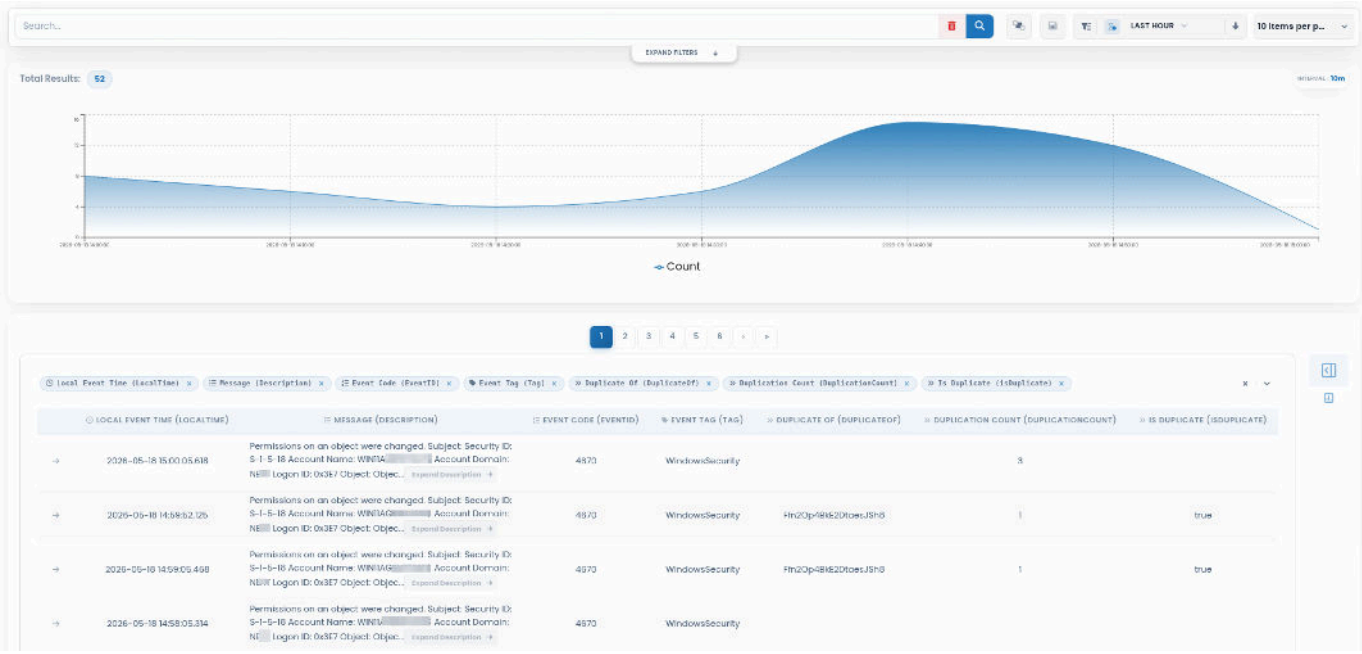
   button.
3. Choose **Add Deduplicate Item**.
4. Select another event that should be marked as a duplicate.
5. Click the

button again.

6. Choose **Set Deduplicate Of**.
7. Select the reference event from the deduplication list.

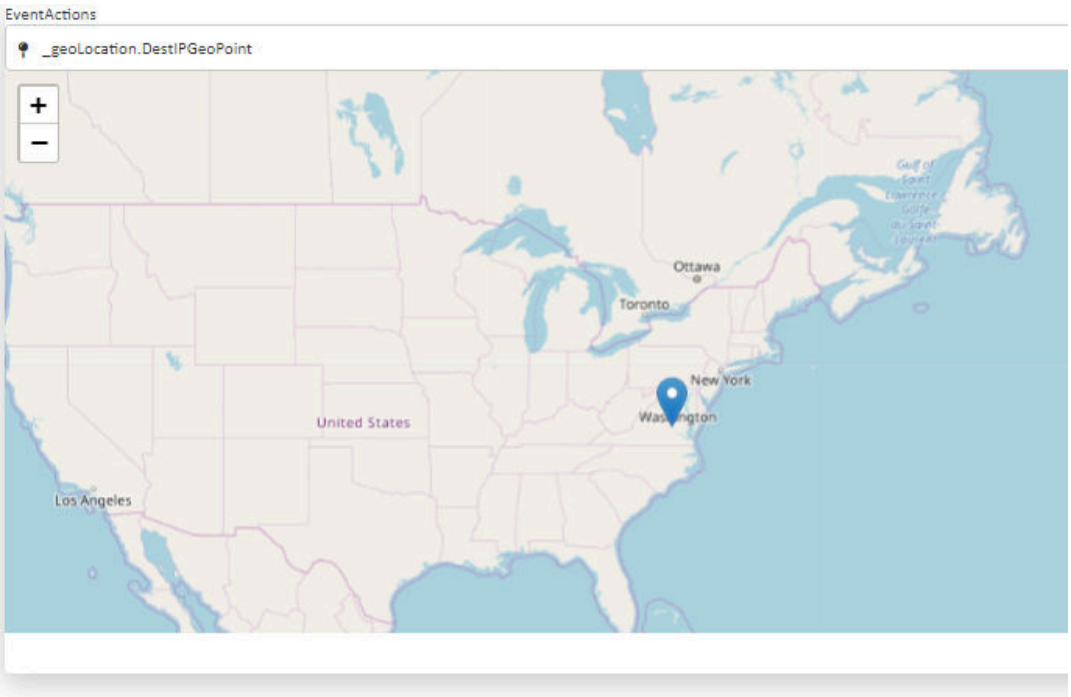
After the deduplication is applied, the event table displays the updated deduplication information:

- **Duplicate Of** - shows the ID of the reference event.
- **Duplication Count** - shows how many events are grouped under the same reference event.-
- **Is Duplicate** - indicates whether the event is marked as a duplicate.



Geolocation section

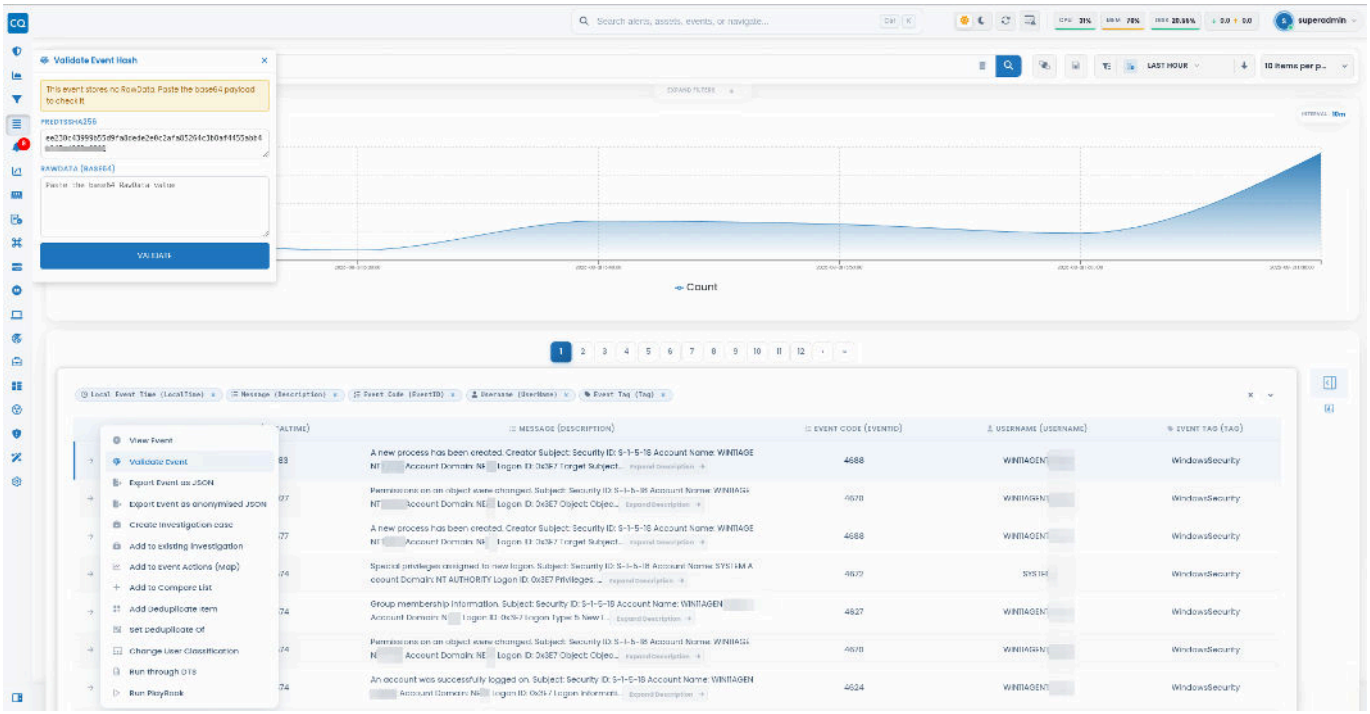
When an event containing a public IP address with geolocation data is added to the map via the Browser, it will be pinpointed on the world map. This feature enables users to visualize the precise origin or destination of the event.



How to validate event integrity

1. In the **Browser** module, locate the event to be verified.
2. Open the event actions menu and select **Validate Event**.
3. The **Validate Event Hash** panel displays the SHA-256 value associated with the event.
4. If the raw payload is available, paste it in Base64 format into the RawData field.
5. Click **Validate** to verify the payload against the stored hash.

Note: *If RawData is not stored with the event, CYBERQUEST displays a notification and allows the original Base64 payload to be provided manually for validation.*

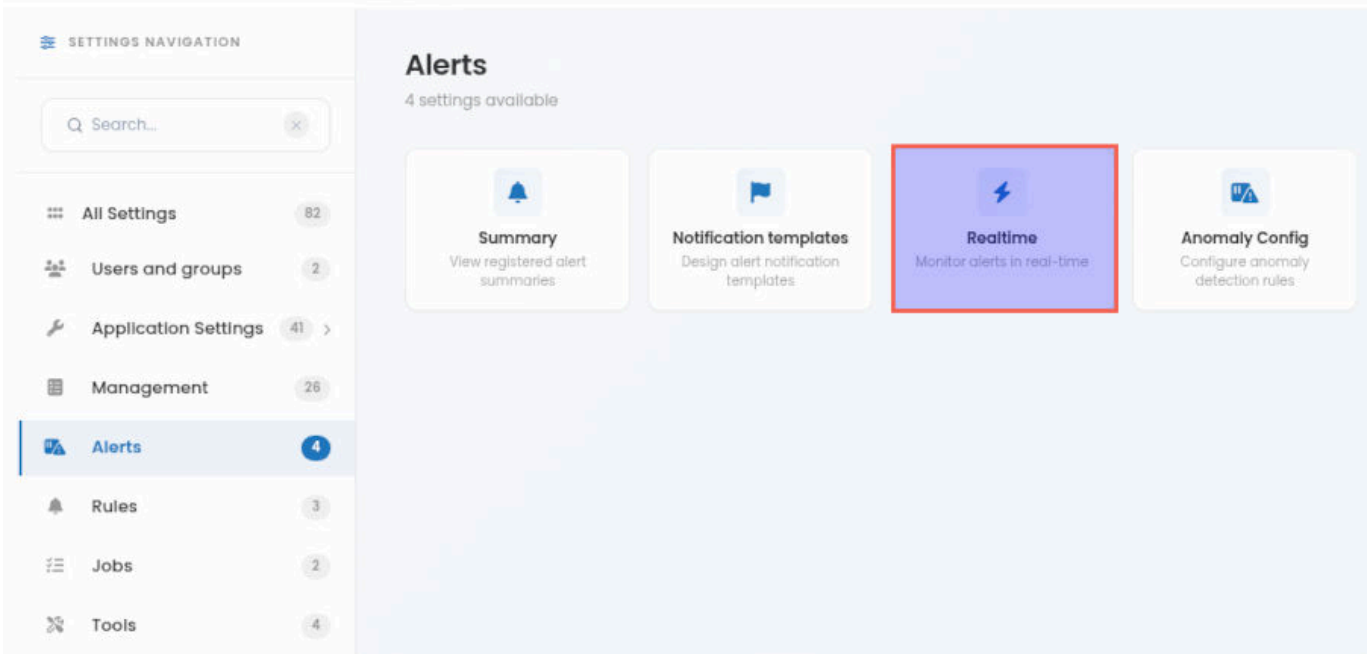


Alerts Module

Creating alerts

Introduction to Alerts Module

The Alerts Module in CYBERQUEST provides a flexible and customizable system for monitoring events. Users can define specific criteria to trigger alerts tailored to their needs, enhancing accuracy and minimizing false positives. Alert configurations are managed through the **Alerts** section in the **Settings** menu.



Customization settings for each option are explained in the following sections.

How to create new alerts

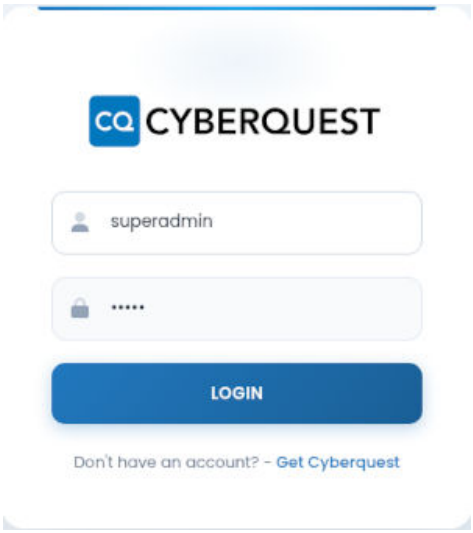
This section outlines the process for setting up new alerts within CYBERQUEST. Defining custom alert criteria enables proactive monitoring of critical events and timely response to potential security issues. The following steps guide the configuration of alerts tailored to organizational needs.

To create a new alert, follow these steps:

Step 1. Authentication

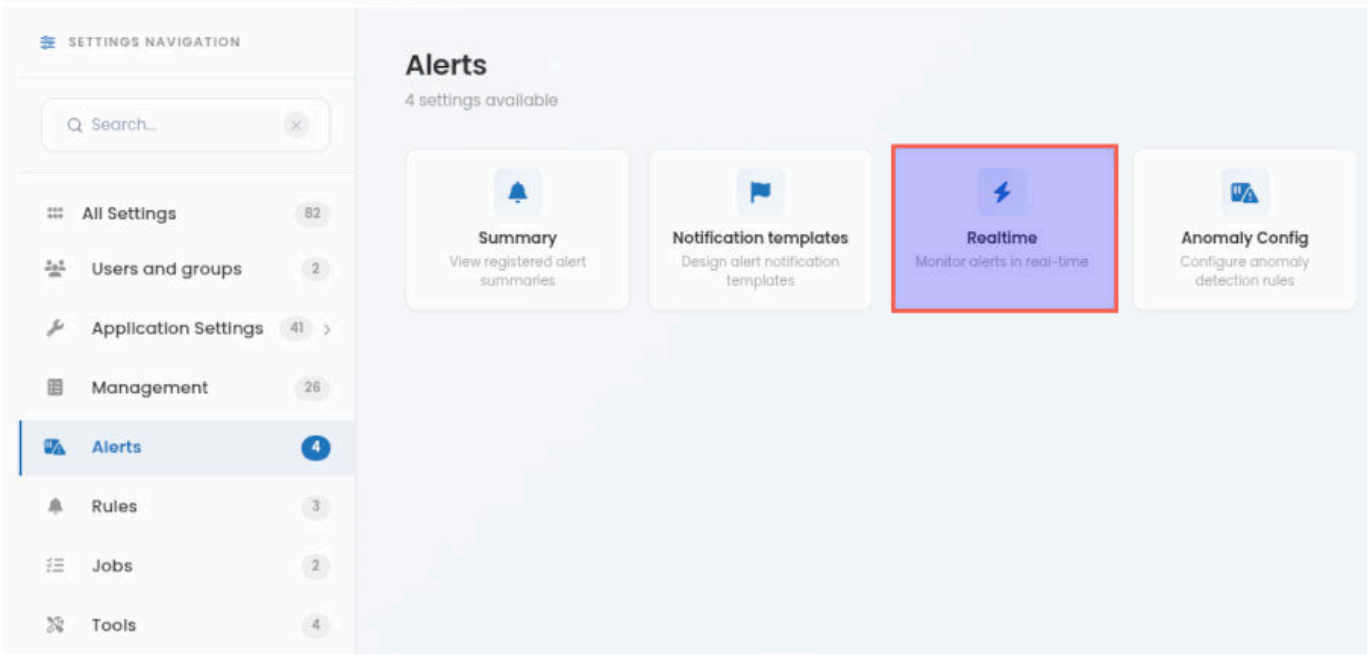
Open a web browser and enter the application's address or DNS name. By default, the Web Interface is accessible at ***https://CyberquestIPAddress*** (example).

The browser will then redirect you automatically to CYBERQUEST's authentication page:



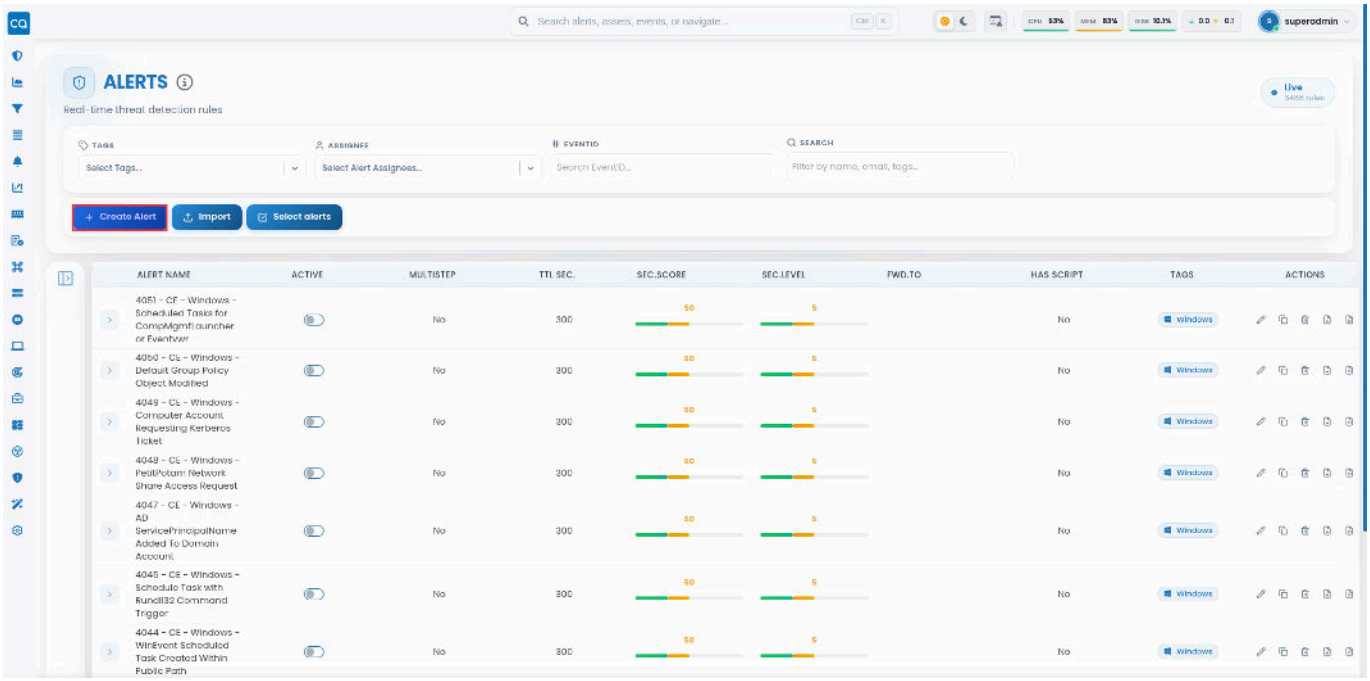
Step 2. Navigate to Alerts

Navigate to the **Settings** menu and select **Alerts > Realtime**. The **Alerts** customization page will open within the **Alerts** module interface.



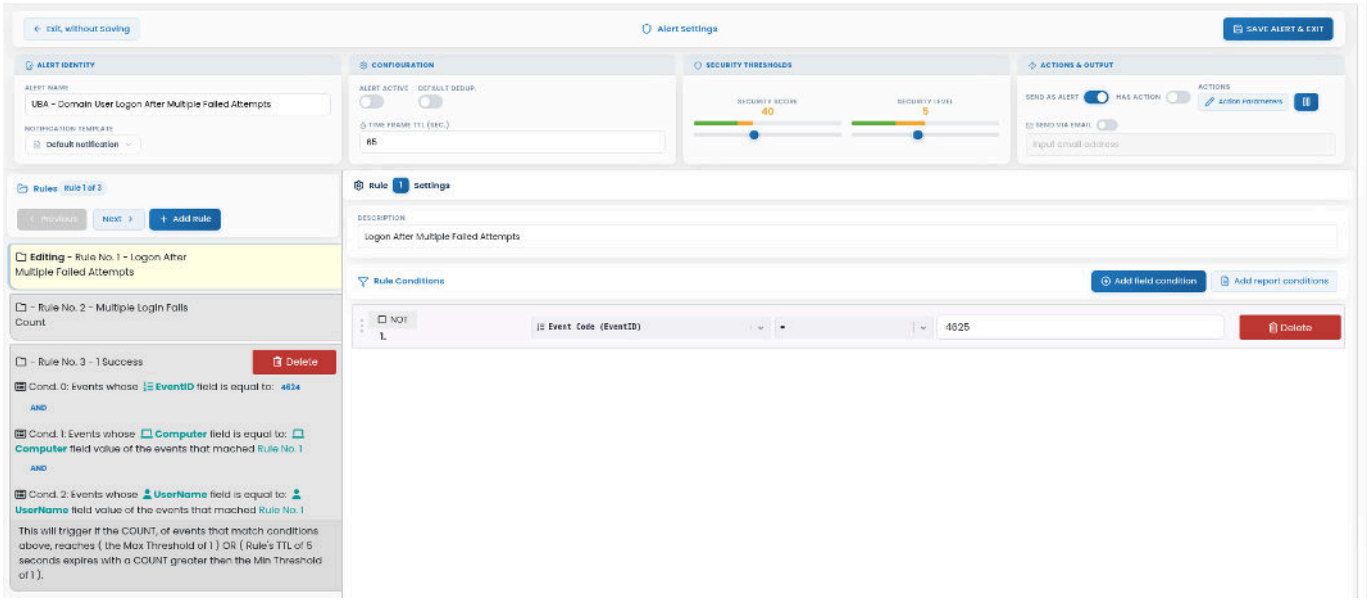
Step 3. Create new alert definition

On the “Alerts” page, select the “Create new alert definition” button to create a new alert.



Step 4. Complete the form

Complete the form with the appropriate information and press “Save Alert & Exit” button:



Alert Name: Specifies the name of the new alert.

Alert Active: Enable the **ALERT ACTIVE** checkbox to activate the alert, or disable it to deactivate the alert.

Default Deduplication: This toggle enables or disables automatic deduplication for the alert. When activated, the system will suppress duplicate alert triggers based on repeated or similar event patterns within the same rule logic. This helps prevent multiple alerts from being raised for the same root cause. When deactivated, all matching events will trigger alerts individually, regardless of duplication.

Time Frame TTL(sec.) : Defines the duration (in seconds) for which the alert remains active after being triggered.

Security Score: Sets the baseline security score for the alert when triggered. The actual real-time score adjusts dynamically based on defined rules and the number of related events, but cannot fall below the baseline or exceed 100.

Security Level: Functions similarly to the security score, with matching color coding to indicate severity levels.

Sent as Alert: When unchecked, the alert remains active but does not generate visible notifications. This option allows backend correlation of anomaly analysis across multiple events, triggers, and alerts. It behaves similarly to the **ALERT ACTIVE** checkbox.

Enable the **Has Action** checkbox to associate the alert with either a script or predefined automated actions. Only one custom script can be created and applied, and it is always evaluated last, overriding other rules in the alert logic.

Enables configuration of alert **deduplication** when **Has Action** is active. Alerts are grouped based on selected fields and a defined time interval.

Send via Email: Enable this checkbox to send the alert notification via emailto defined recipients.

Notification Template: Select a notification template for the alert. Options include built-in and custom templates. The default selection is “Default notification.”

Rules Section

Rules define the detailed behavior of the alert, ranging from single event conditions to complex correlations between multiple events, including event order, correlation to missing an event from a logical succession of events.

- **Previous:** Navigate to the previous alert condition.
- **Next:** Navigate to the next alert condition.
- **Add Rule:** Adds a new rule. The rule is configured in the Rule Settings pane on the right.

Rule Settings Pane

This pane facilitates defining the logic of each rule. Rule logic consists of field, report, and correlation conditions combined using logical operators **AND**, **OR**, and **NOT**.

Each rule includes:

- **Description:** Provide details about the rule's behavior or the conditions it monitors.
- **Add field condition:** elect an event field from the drop-down menu, choose the appropriate operator, and enter the value to compare.
- **Add report condition:** Select a report from the drop-down list of existing reports to include as a condition.
- **Delete:** Remove a specific rule condition.

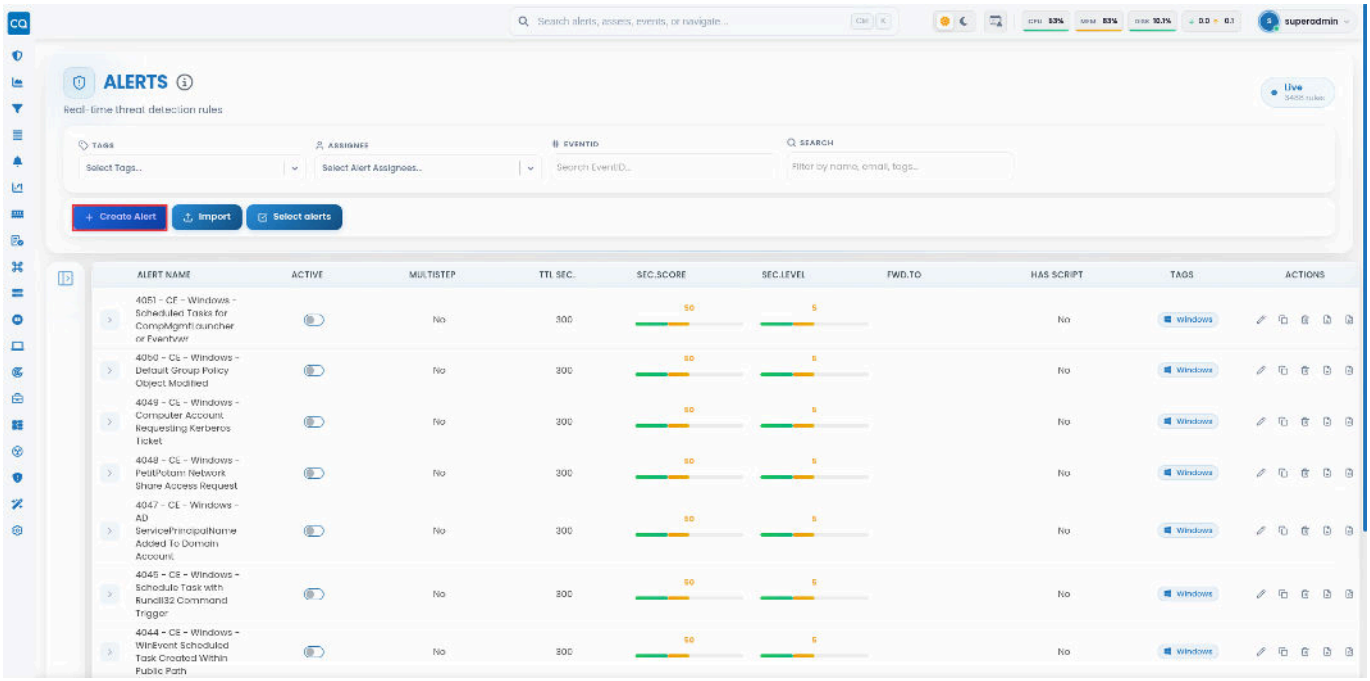
When adding rule conditions, a logical operator is automatically inserted to correlate the new condition with the previous one. The default operator is **AND**. Click the **AND** switch to toggle between **AND** and **OR**.

If needed by the logical chain, a **NOT** operator is available as a checkbox. It is unselected by default. Click **NOT** to enable the operator.

Real time alerts

Real time alerts customization

To access real-time alert settings, go to **Settings > Alerts > Realtime**. This opens the **Alerts** customization page within the **Alerts** module. All existing alert definitions are displayed and can be edited, deleted, cloned, or exported as a CQO or XML.



Click the "***Create Alert***" button to create a new alert definition. The **Alert Settings** window will open, enabling the creation of a custom alert tailored to specific requirements. This window has the same features as the alert editing interface, which is detailed later in this chapter.

At the top of the page, a drop-down list labeled **Select Tags** allows filtering alert definitions by categories

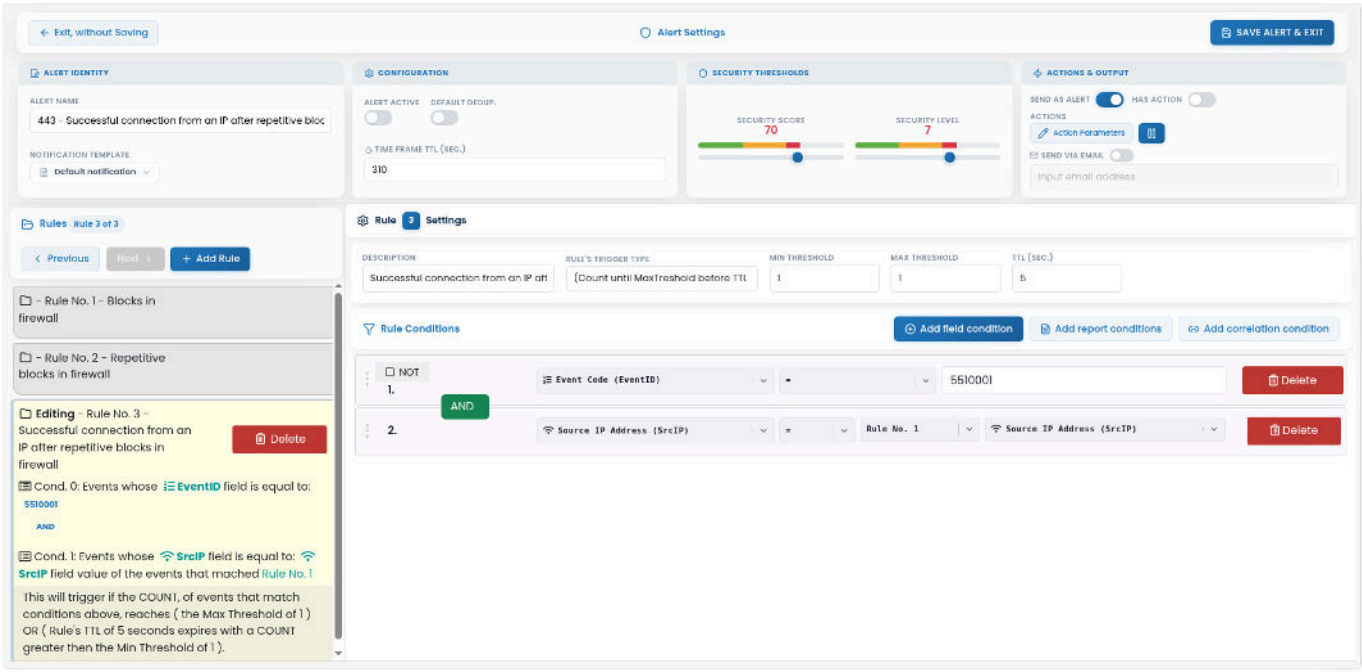
A drop-down filter at the top of the page that displays **alerts assigned** to a specific user or team, helping to quickly identify and manage alerts based on ownership.

At the bottom of the page, a navigation selector enables browsing through pages with alert definitions.

Editing an alert definition

Press

button to edit an existing definition. **Alert Settings** window opens:



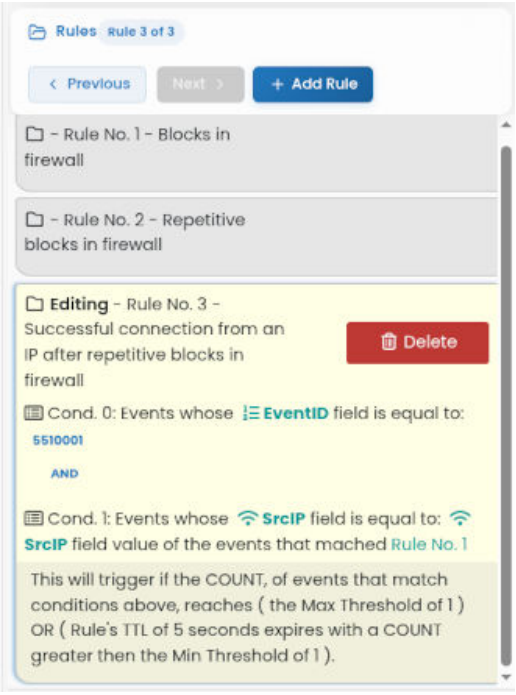
Under **Alert Name** section, you can set the following options:

- Enter an alert name, change or leave unchanged.
- **Notification Template:** Select a notification template for the alert. Options include built-in and custom templates. The default selection is “Default notification.”
- **Alert Active:** Enable the **ALERT ACTIVE** checkbox to activate the alert, or disable it to deactivate the alert.
- **Default Deduplication**: This toggle enables or disables automatic deduplication for the alert. When activated, the system will suppress duplicate alert triggers based on repeated or similar event patterns within the same rule logic. This helps prevent multiple alerts from being raised for the same root cause. When deactivated, all matching events will trigger alerts individually, regardless of duplication.
- **Time Frame TTL(sec.) :** Defines the duration (in seconds) for which the alert remains active after being triggered.
- **Alert Security Score:** Sets the baseline security score for the alert when triggered. The actual real-time score adjusts dynamically based on defined rules and the number of related events, but cannot fall below the baseline or exceed 100. Security Score Color Codes:
  - **Green - Represents a low-severity alert, with a score up to 30**.
- **Yellow** - Indicates a medium-severity alert, with scores ranging from **31 to 60**.
  - **Red** - Denotes a high-severity alert, with scores between **61 and 100**.
- **Alert Security Level:** Functions similarly to the security score, with matching color coding to indicate severity levels.
- **Sent as Alert:** When unchecked, the alert remains active but does not generate visible notifications. This option allows backend correlation of anomaly analysis across multiple events, triggers, and alerts. It behaves similarly to the **ALERT ACTIVE** checkbox.
- Enable the **Has Action** checkbox to associate the alert with either a script or predefined automated actions. If automated actions are configured in the alert, they will execute only after all rule conditions within the alert definition have been fulfilled. These actions represent the final response stage triggered by the alert logic.

- Enables configuration of alert **deduplication** when **Has Action** is active. Alerts are grouped based on selected fields and a defined time interval.
- **Send via Email:** Enable this checkbox to send the alert notification via emailto defined recipients.

  For additional details on configuring Action Parameters, refer to: How to activate automatic Actions in Realtime Alerts

Under the **Rules** section, alert behavior can be precisely defined using granular rule configurations. This includes single-event rules, correlations between multiple events, event sequence logic, and detection of missing events within an expected pattern.



The left pane displays the list of defined rules. The following actions are available:

- To add a new rule, click the

  button. The rule will appear in the **Rule Settings** pane on the right.
- Use the

  buttons to navigate through the existing rules. The currently selected rule is highlighted in yellow, and its configuration is displayed in the Rule Settings pane
- To remove a rule, click the

  button.

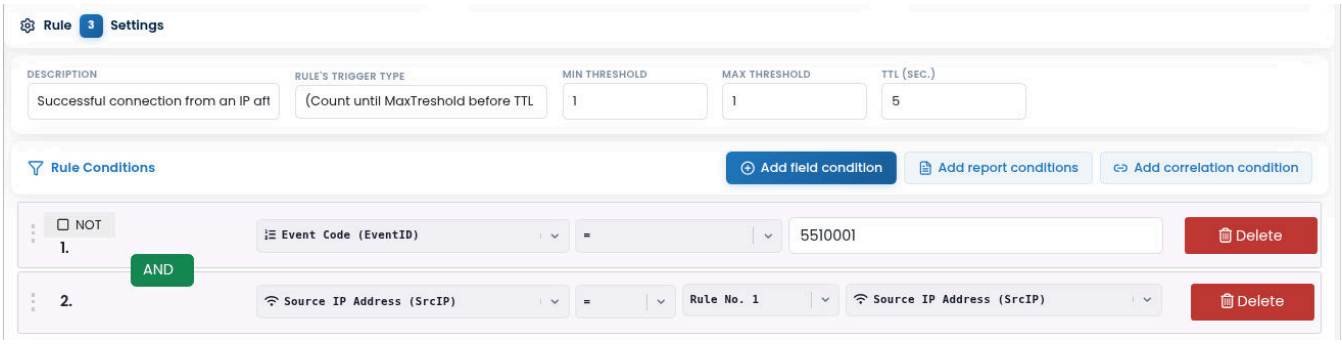
The Rule Settings pane is used to define the logic behind each alert rule. Rule logic consists of field conditions, report conditions, and correlation parameters, combined using the logical operators AND, OR, and NOT.

Each rule includes the following elements:

- **Description**: A text field for detailing the purpose or behavior of the rule.
- **Rule Trigger Type**: A drop-down menu offering several trigger types

- Single Event Trigger - activates the alert when a single event meets the defined conditions. No threshold or accumulation is required.
- Count until MaxThreshold (the maximum number of events counted) before TTL value expires, or TTL expires and count MinThreshhold (the minimum number of events counted) value is achieved - how many *(for e.g. 3 customers with 25% discount if you group by discount)*
- Sum PivotField (the arithmetic sum for a specific field) until MaxThreshold (the maximum amount) before TTL value expires or TTL expires and Sum PivotField MinThreshold (the minimum amount) value is achieved - how much *(for e.g. for business applications: if the total value discount for region is more than 1000 euro)*
- Average on PivotField until TTL has MinThreshold value
- (Distinct values on PivotField until MaxTreshold before TTL expires) OR (TTL expires and Distinct values count on PivotField MinTreshold achieved) - number of distinct values *(for e.g. how many distinct IP addresses send events, made attack for specific field)**

- **MaxThreshold**, **MinThreshold**, and **TTL (sec.)** values for the rule's trigger type



MaxThreshold - the maximum number of events required to trigger the alert.

MinThreshold - the minimum number of events required to trigger the alert.

PivotField - the sum of a specific field *(e.g., total monetary value or number of transactions in business applications)*

Rule conditions can be added, edited, or deleted as follows:

- To add a field condition, press the

  button. In the **Select Field** drop-down, choose a relevant event field. Then, select the appropriate value operator from the next drop-down, and enter the corresponding value in the third field.
- To add a report condition, press

  button. A drop-down list will appear, allowing selection from all existing reports.
- To add a correlation condition, press

  button. This opens two **Select Field** drop-downs for selecting event fields to correlate, a **comparison operator** drop-down—providing options such as `equal`, `not equal`, `less than`, `less than or equal`, `greater than`, `greater than or equal`, along with additional operators like `isInList`, `isNotInList`, `startsWith`, `endsWith`, `contains`, `range`, `containsAnyOf`, `containsAllOf`, and `regexMatch`. A corresponding rule condition can also be selected for the correlation to apply.

The script rule is evaluated last in the sequence of rule conditions and, together with any configured automated actions, is executed only after all other alert rule conditions are fullfiled.

To delete a rule condition, press the



button located at the far right of the rule condition entry.

When adding a new rule condition, a logical operator is automatically inserted to correlate it with the previous condition. The default operator is AND. Click the



toggle to switch the operator to OR; click again to revert to AND.

If required by the logic structure, a **NOT** operator is also available as a checkbox. By default, it is not selected. Click



to enable it. The resulting logical expression will be interpreted as **AND NOT**.

All rule conditions are added sequentially, in the order they are defined.

Once configuration is complete, click the



button at the top to save the rule and return to the alert definitions list. To discard all changes, click the



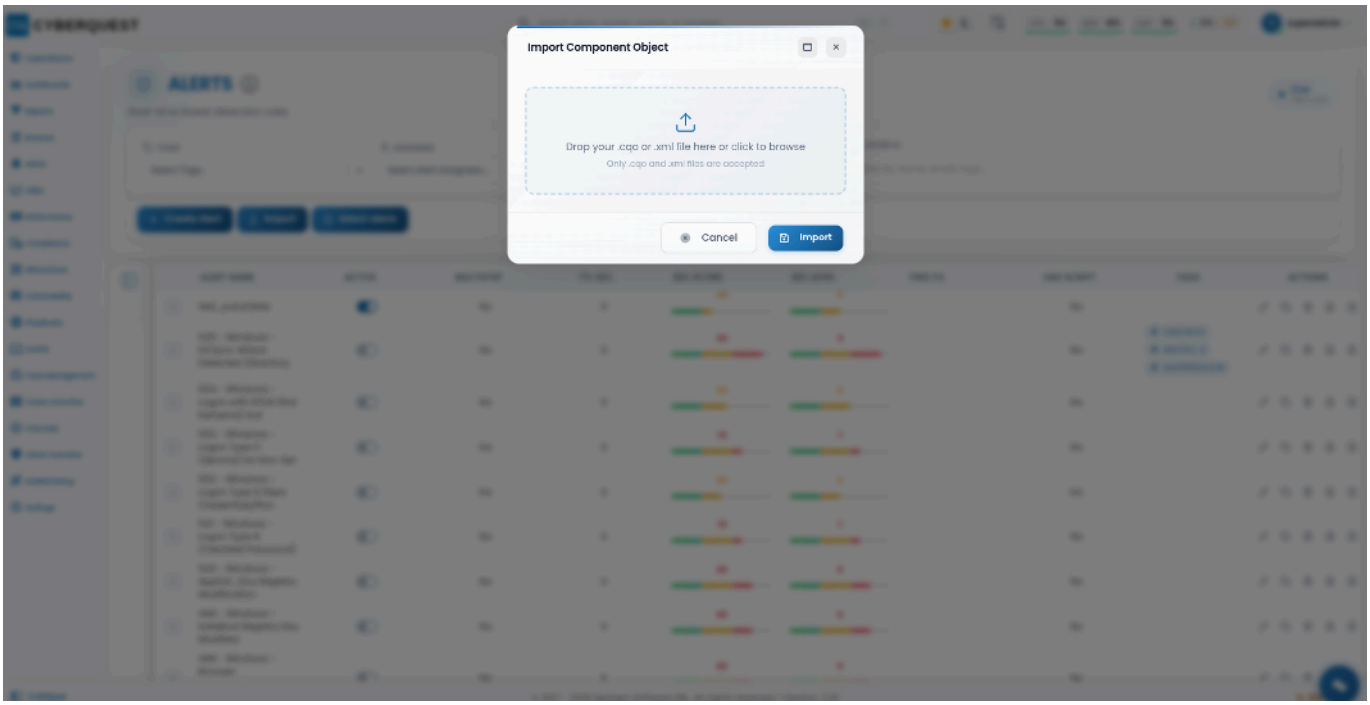
button.

Example of a script rule:

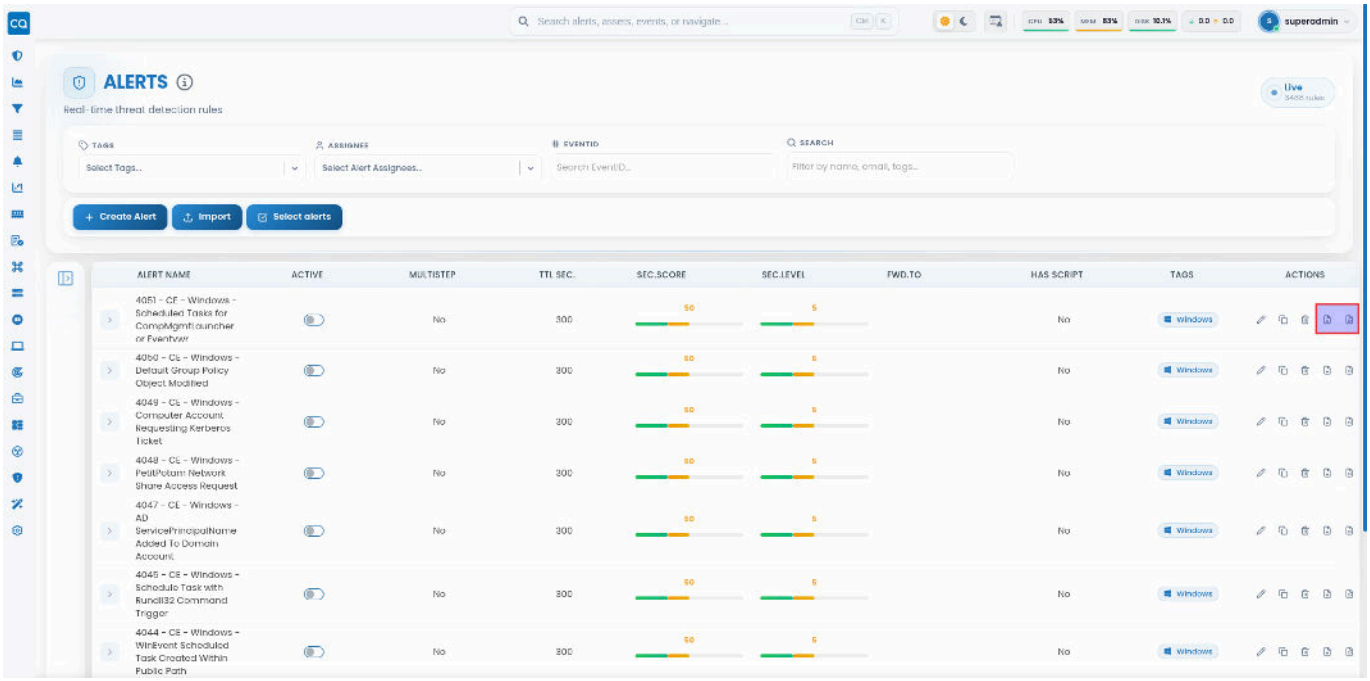
```
   var currentAlertState =  JSON.parse(Alert);
   return false; // triggers current alert instance supression. If return is NOT used, the alert is not triggered as
well.
```

Import and export realtime alert definitions

Realtime alert definitions can be imported and exported directly from the graphical interface. Click **Import** to import an existing alert definition from an `.xml` or `.cqo` file.



To export an alert definition, use **Export Object** for the CYBERQUEST `.cqo` format or **Export XML** for the XML format, using the corresponding action available in the alert row.



Alert Deduplication

Alert deduplication is a mechanism that consolidates multiple alert instances triggered by identical or similar event patterns within a specified time interval. It helps optimize alert handling by preventing redundant alert generation for recurring conditions that match the same rule logic.

To access the deduplication settings, the **Has Action** option must be enabled. Once enabled, the **Duplicate** button



becomes available and can be used to access the deduplication configuration.



Configuration options include:

- ***Interval***: Defines the time window during which similar alerts are grouped and treated as a single occurrence. Available options include 1 minute, 10 minutes, 1 hour, and 1 day.
- ***Deduplication fields***: Specifies the fields used to determine if alerts are considered duplicates. These fields must be configured so CYBERQUEST can accurately group alerts based on matching criteria.
- When duplicate alerts are detected within the specified interval and fields, the alert count is incremented, and the LastSeen timestamp is updated accordingly.

Once configuration is complete, **Set** saves and applies the deduplication settings, while **Cancel** discards any changes and closes the configuration window.

Manual alert deduplication is also available to mark duplicates: Alerts Manual Deduplication

Create a Logon alert scenario example

This scenario outlines how to configure an alert that triggers when a specific user experiences two failed logon attempts within a 60-second interval.

Step 1: Navigate to **Settings > Alerts > Realtime**.

To create a new alert, click the **CREATE ALERT** button on the **Alerts** page.

Step 2:

Configure the alert definition with the following settings:

- **Name:** Default - Audit policy change
- **Alert Active:** Enabled
- **Send as Alert**: Enabled
- **Security Score:** 40
- **Security Level:** 5

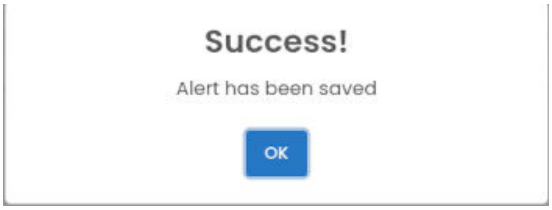
Step 3:

Add a new rule with these parameters:

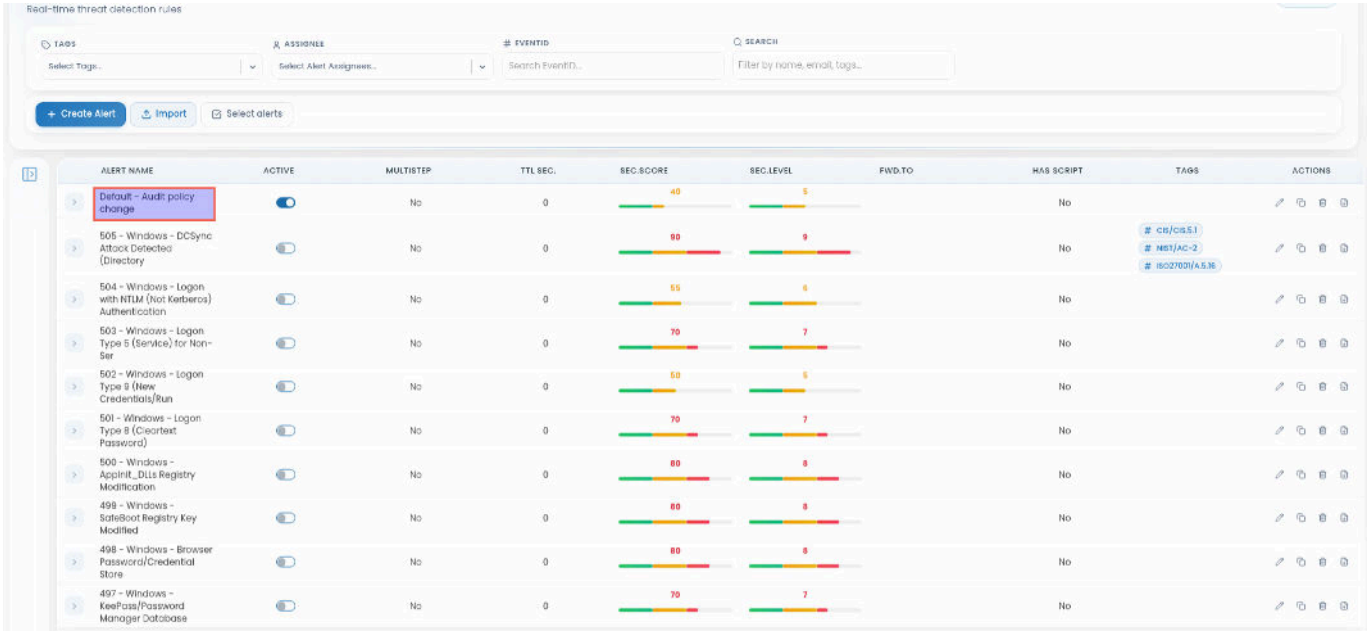
- **Description:** Audit policy change events
- **EventID:** 4719 *Note: Event IDs can be referenced in the* Event Dictionary

Step 4:

Save the alert definition.



The new alert will now appear listed on the **Alerts** page.



Step 5:

When conditions are met - specifically, when two failed logon attempts by the specified user occur within 60 seconds - an alert is generated in real time. This alert corresponds to Event ID 4719 (Audit policy change) retrieved from the Windows Security Log and is visible in the Alerts module interface.

How to activate automatic Actions in Realtime Alerts

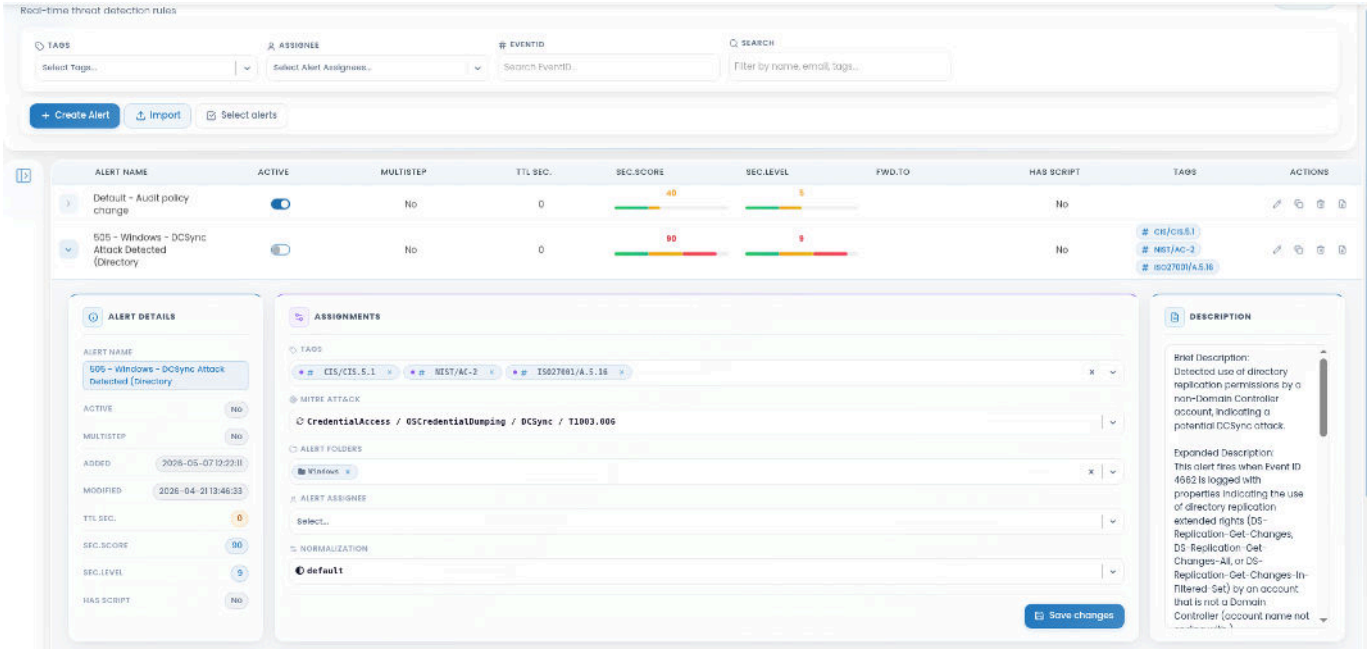
To use predefined automatic actions, explore the available configurations and setup guides in the How to activate automatic Actions in Realtime Alerts.

For instructions on creating a new alert, please refer to the provided link: How to create new alerts

Alert Detail Properties

Clicking the

icon in the **Alert Name** column opens the **Alert Viewer** pop-up, where detailed alert information and configuration options are available for review and adjustment.



Alert Summary Panel

This panel provides a quick overview of the alert's key metadata, including the alert name, creation and modification timestamps, security score and level:

- **Alert Name -** Displays the name of the alert. Example: *UBA - User Logon from Multiple IP Addresses*.
- **Added -** Shows the date and time when the alert was created or added to the system.
- **Modified -** Indicates the last date and time when the alert configuration was updated.
- **Sec. Score -** Displays the calculated **Security Score**, a numerical value that reflects the severity or impact level of the alert based on predefined scoring rules.
- **Sec. Level -** Represents the **Security Level**, a simplified classification of alert severity (e.g., from low to critical), determined by the system based on scoring thresholds.

Alert Configuration Panel

This panel allows further classification and contextualization of the alert. Users can assign tags, associate the alert with MITRE ATT&CK techniques, specify alert folders, assign ownership, and view normalization settings.

- **Tags -** Allows assigning custom tags to the alert, enabling efficient categorization, filtering, and management based on operational context or threat attributes. Tagging can support compliance and reporting requirements aligned with standards such as **ISO 27001**, **NIS2**, **NIST 800-53**, **GDPR**, and **CIS Control V8**, by helping classify alerts according to security controls, data types, or regulatory impact.
- **MITRE ATT&CK -** Allows mapping the alert to a corresponding MITRE ATT&CK tactic or technique. This supports alignment with industry-standard threat intelligence and aids in threat classification.
- **Alert Folders -** Lets users organize the alert into specific folders for easier management, access control, or workflow segmentation.
- **Alert Assignee -** Assigns responsibility for the alert to a specific user. This helps with task ownership and facilitates alert triage and resolution.
- **Normalization -** Displays the applied normalization profile. This defines how raw event data is standardized to a consistent schema, enabling effective correlation and analysis.

Alert Normalization

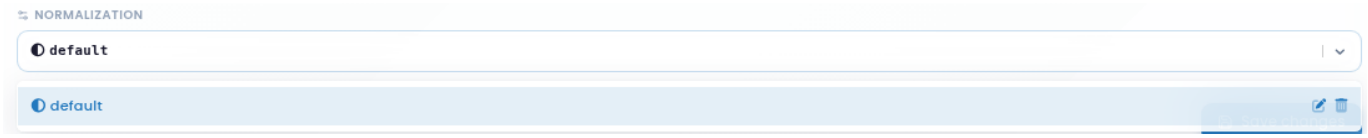
Alert Normalization ensures consistency across alerts by assigning predefined values to specific fields. This process simplifies alert categorization, integration with external systems, and compliance with organizational or regulatory standards.

Normalization is especially useful when alerts originate from various data sources with differing formats. By mapping fields to standardized values, alerts become easier to correlate, filter, and report.

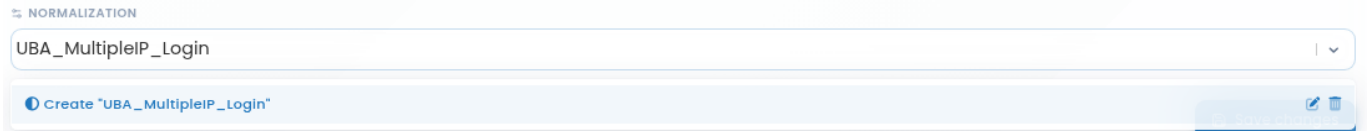
Accessing Normalization Settings To configure normalization:

- Navigate to the **Normalization** section.
- In the dropdown list, a default normalization profile is displayed (named `default`).

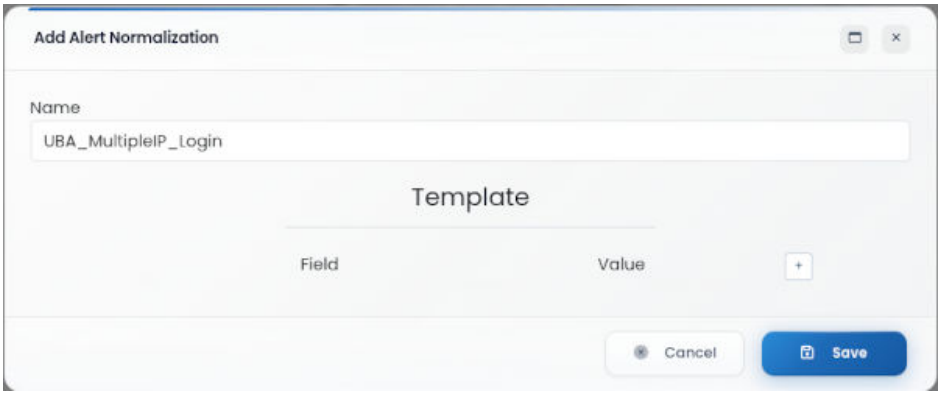
***Note**: The default profile is not editable.*



- To **create** a custom normalization, type a new name in the input box below the dropdown.

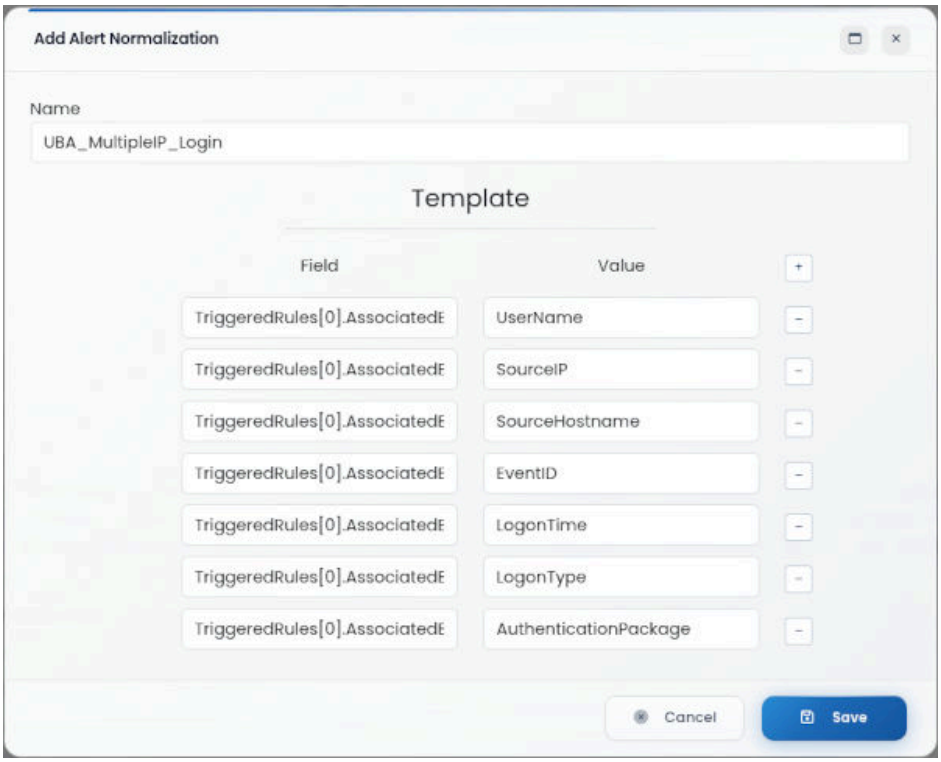


- Clicking the newly entered name opens the Add Alert Normalization interface for customization.



- Click the

button to add field-to-value mappings for alert normalization.



Name: Specifies the name of the normalization profile (e.g., `default`). It identifies the configuration applied to alerts when normalization is triggered.

Field: The path to the actual data within the alert structure (e.g., `TriggeredRules[0].AssociatedEvents[0].UserName`).

Value: Specifies the normalized label (e.g., `UserName`, `SourceIP`, `LogonTime`) that will represent this data in a standardized format.

Once the configuration is complete, click **Save** to apply the alert normalization settings. To discard any changes and close the configuration window, click **Cancel**.

- Options are available to **edit** or **delete** the *alert normalization* configuration.

Summary alerts

Summary alerts customization

Summary alerts are used to group historical event data based on defined conditions within reports.

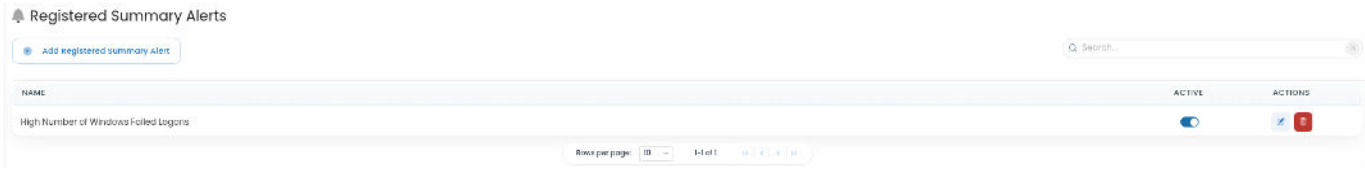
For example, when using CYBERQUEST to monitor business applications, summary alerts can be configured to group discount values by country or other relevant fields.

Unlike real-time alerts, which are generated instantly by the Data Correlation service as events are ingested, summary alerts operate on processed historical data. These events are aggregated every 10 minutes and can be grouped using custom-defined keys for statistical analysis.

To manage summary alerts, navigate to **Settings > Alerts > Summary**. This opens the **Registered Summary Alerts** page, where you can:

- View all configured summary alerts
- Create new summary alert definitions
- Edit or delete existing alerts
- Toggle alert activation status (active/inactive)

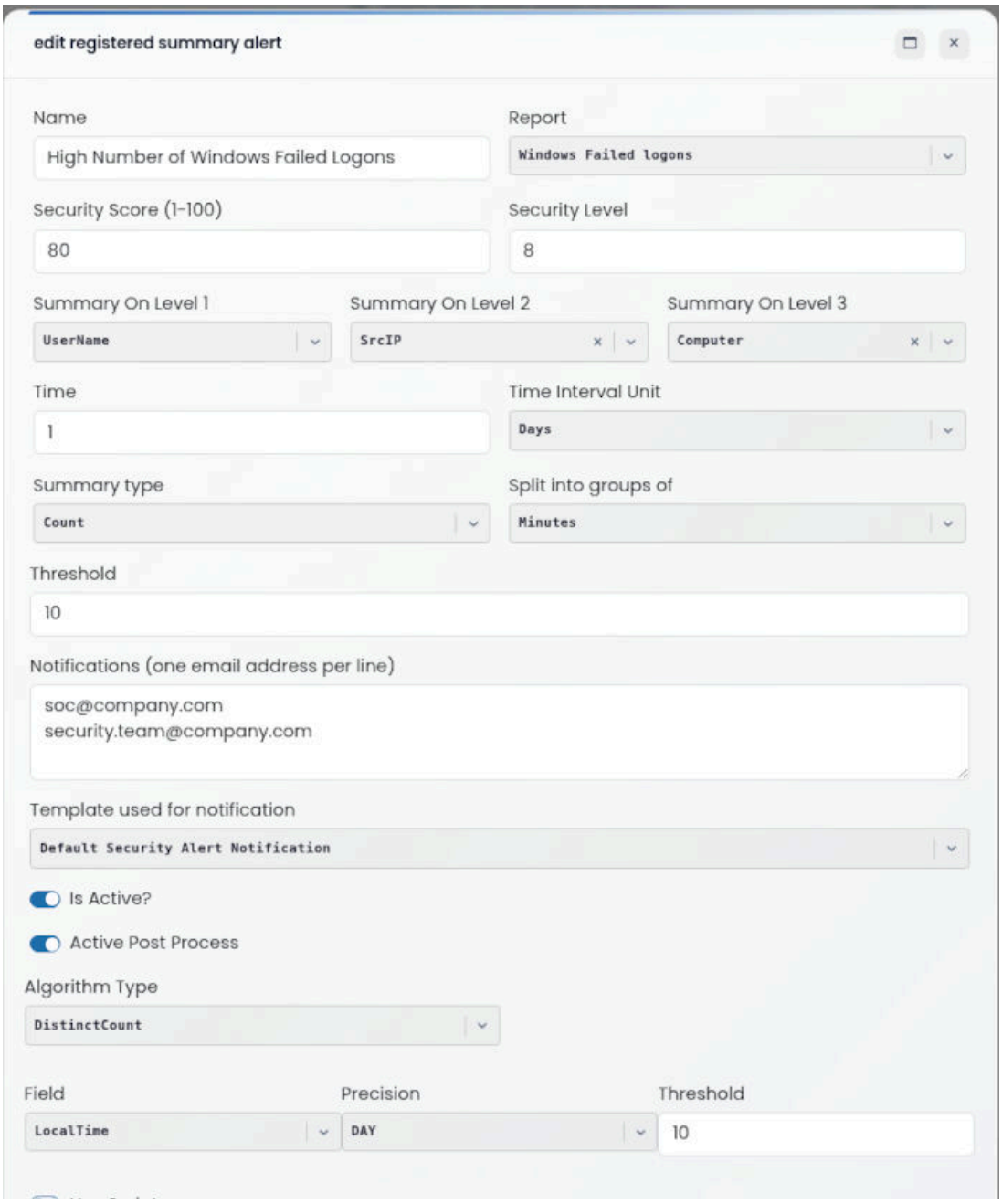
The **Actions** menu provides quick access to these management options for each alert entry.



Click the



button, to modify the alert. Below is a detailed overview of each configuration available on the **Edit registered summary alert** page:



- **Name** - Displays the name of the registered summary alert.
- **Report** - indicates the report for which current summary alert is generated
- **Security Score and Security Level** - Define the baseline risk level associated with this summary alert. These values contribute to internal anomaly scoring, as also used in real-time alert definitions.

- **SummaryOn Level n**, **Time**, **TimeInterval Unit**, **Summary Type**, **Split Into Groups of**, and **Threshold** – Parameters used to define how data is grouped and evaluated for the summary alert.
- **Notifications** - Specifies the recipient email addresses for alert notifications. Enter one address per line without separators.
- **Template Used for Notification** - Drop-down menu listing available templates for formatting email notifications.
- **Is Active?** - Specifies whether the summary alert is currently enabled.
  - *Active - The alert is running and will generate summary events based on the defined conditions.*
  - *Inactive - The alert is turned off and does not evaluate or generate any summary results.*
- **Active Post Process** - This section allows you to define post-processing logic for the summary alert, applying additional filtering or evaluation through a simple algorithm. When enabled, the following configuration fields appear:
  - **Algorithm Type** - Drop-down list with available post-processing algorithms.
  - **DistinctCount** - Counts the number of distinct values in a specified field within the alert's summary dataset.
  - **Field** - The field on which the algorithm operates (e.g., `LocalTime`).
  - **Precision** - Defines the level of time granularity for evaluation.

    Available options:

    HOUR - Group results per hour.

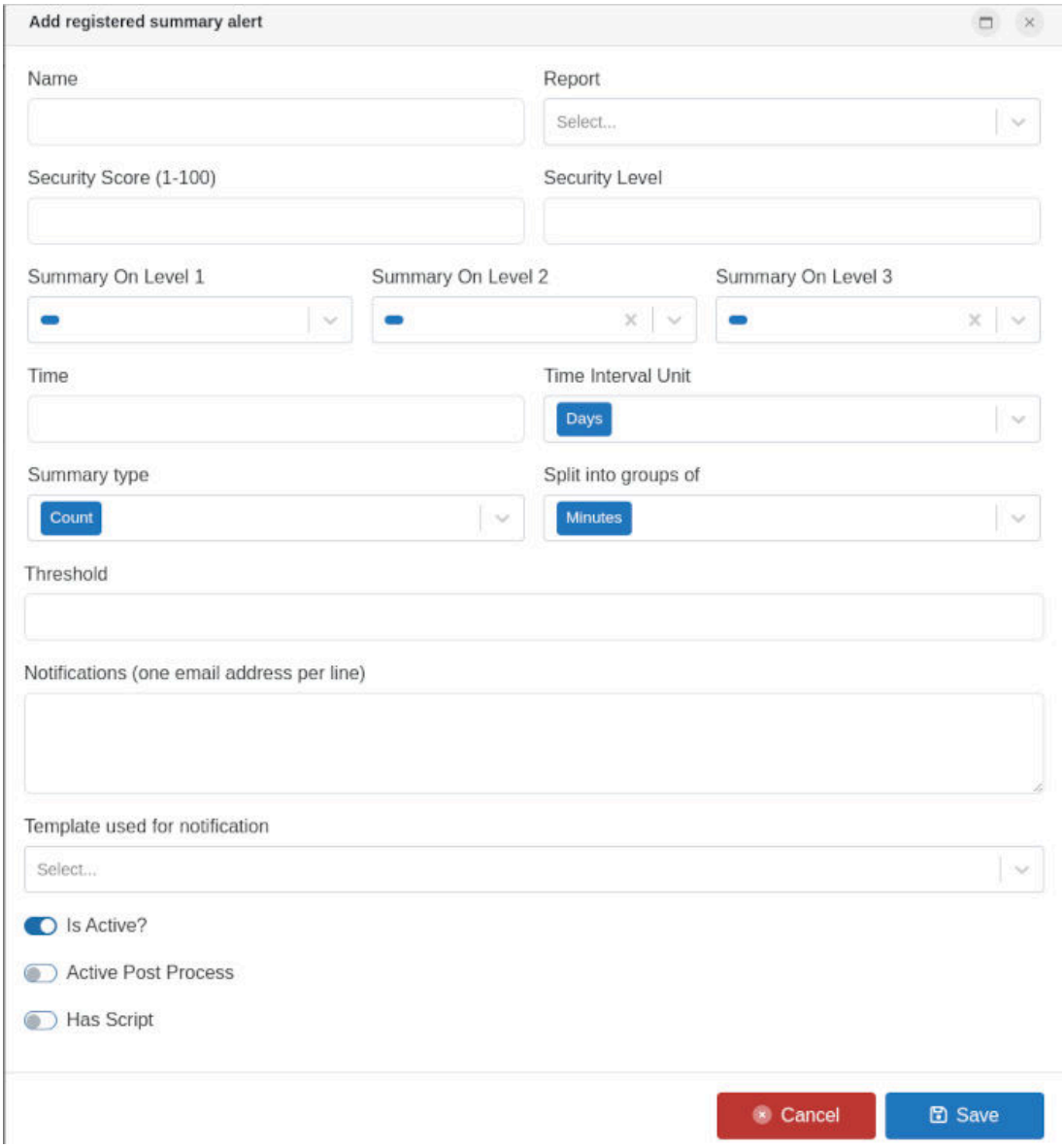
    DAY - Group results per day.
  - **Threshold** - The minimum value required to trigger the post-processing condition.

    Example: `10` means the condition is met if there are 10 or more distinct values based on the selected field and precision.
- **Has Script** - Specifies whether a custom script is associated with the alert.
  - **Enabled** - A script is attached and will be executed as part of the alert's processing workflow.
  - **Disabled** - No script is assigned to the alert.

Press the **Save** button to save changes and return to the **Registered Summary Alerts** page, or press the **Cancel** button to discard changes and exit without saving.

Creating a new registered summary alert

To create a new summary alert, select the **Add Registered Summary Alert** option available on the pages mentioned above. This will open the **New Summary Alert** page, where the available settings are similar to those described in the **Edit Summary Alert** section.



- Enter a unique name for the new summary alert in the **Name** field.
- From the **Report** drop-down list, select the report for which the summary alert will be generated.
- Specify baseline values for the summary alert's security threat in the **Security Score** and **Security Level** fields. If unsure, a default value of 50 for Security Score and 5 for Security Level is recommended.
- In the **SummaryOn Level *n*** drop-downs, select the event fields to summarize. At least a value for Level 1 is required for the summary alert to function.
- Set the **Time** value and corresponding **TimeInterval Unit** (minutes, hours, days, weeks, months, quarters, or years) to define the time window for the summary- counting backward from the current moment (e.g., 3 days ago).
- Choose the **Summary Type** (count, sum, or average) based on the required aggregation.
- Define the **Split Into Groups of** value to determine how results are grouped. The default grouping is by minutes.
- Enter a **Threshold** value representing the maximum number of grouped events that will trigger the alert (e.g., 1000 for a region).
- In the **Notifications** field, list email addresses for summary alert delivery, one address per line without separators.
- Optionally, select a **Template Used for Notification** to format the alert message.
- **Is Active?** - Determines if the summary alert is enabled.
  - *Active: The alert runs and generates summary events.*
  - Inactive: The alert is disabled and not evaluate or generate any summary result
- **Active Post Process** - Enables additional filtering or evaluation using a selected algorithm on the summary data. Configure *algorithm type*, target *field*, *precision* (hour/day), and *threshold* to control how the post-processing affects alert triggering.

- **Has Script** - Indicates if a custom script is linked to the alert.
  - *Enabled: Script runs during alert processing.*
  - *Disabled: No script assigned.*

Press the **Save** button to save changes and return to the **Registered Summary Alerts** page, or press the **Cancel** button to discard changes and exit without saving.

Configuring a Logon summary alert scenario example

This scenario notifies the security officer when a user fails to authenticate more than 50 times within a day.

Step 1: Create the Report

Develop a report that filters relevant events—in this case, "An account failed to log on." When run, the report will identify all matching events and send notifications containing details such as network address, username, date, and time. To create this report:

- Open the **Browser** module.

  Search for `EventID:4625` (the Windows event ID for "An account failed to log on"). Use **Filter Data** to display matching events.

  Click **Save** and select **Save as New Report**.

  Enter "An account failed to log on" as both the **Name** and **Description**.

  By default, the report will be saved in the **Custom Reports** folder under the **Reports** module.

Step 2: Create the Summary Alert

Create a new summary alert based on the report:

- Navigate to **Settings > Alerts > Summary**.
- Click **New Registered Summary Alert**.
- Configure the following settings:
  - Select the custom report created in Step 1.
  - Set **Security Score** to 50 and **Security Level** to 5.
  - Set **SummaryOn Level 1** to `UserName`.
  - Set **SummaryOn Level 2** to `Computer`.

Step 3: Review Results

Monitor the alert results for triggered notifications.

DTS Alerts

DTS Objects

Data Transformation Service (DTS) enables alert generation by evaluating internal object lists. These objects support operations including log enhancement, data enrichment, decision-making, alerting, and other processing tasks.

A CYBERQUEST event has the following format:

```
{
  "EventID": "1-2000000000",
  "LocalTime": "yyyy-mm-dd hh:mm:ss.fff",
  "GMT": "yyyy-mm-dd hh:mm:ss.fff",
  "UserName": "blacklisted.user1",
  "UserDomain": "Demo",
  "SrcIP": "xxx.xxx.xxx.xxx",
  "DestIP": "xxx.xxx.xxx.xxx",
  "VersionMajor": "6",
  "VersionMinor": "2",
  "Computer": "A-PC.Demo.local",
  "Source": "Microsoft-Windows-Security-Auditing",
  "EventLog": "Security",
  "Category": "Logon",
  "EventType": "8",
  "Description": "An account was successfully logged on.\r\n\r\nSubject:\r\n\tSecurity ID:\t\tS-1-0-0\r\n\tAccount Name:\t\t-\r\n\tAccount Domain:\t\t-\r\n\tLogon ID:\t\t0x0\r\n\r\nLogon Type:\t\t\t3\r\n\r\nImpersonation Level:\t\tImpersonation\r\n\r\nNew Logon:\r\n\tSecurity ID:\t\tS-1-5-21-1009658894-4016096118-1013530418-1275\r\n\tAccount Name:\t\tblacklisted.user1\r\n\tAccount Domain:\t\tDemo\r\n\tLogon ID:\t\t0xC2C9FA762\r\n\tLogon GUID:\t\t{00000000-0000-0000-0000-000000000000}\r\n\r\nProcess Information:\r\n\tProcess ID:\t\t0x0\r\n\tProcess Name:\t\t-\r\n\r\nNetwork Information:\r\n\tWorkstation Name:\tRemoteWorkstation\r\n\tSource Network Address:\t10.10.10.10\r\n\tSource Port:\t\t44214\r\n\r\nDetailed Authentication Information:\r\n\tLogon Process:\t\tNtLmSsp \r\n\tAuthentication Package:\tNTLM\r\n\tTransited Services:\t-\r\n\tPackage Name (NTLM only):\tNTLM V1\r\n\tKey Length:\t\t128\r\n\r\nThis event is generated when a logon session is created. It is generated on the computer that was accessed.\r\n\r\nThe subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.\r\n\r\nThe logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network).\r\n\r\nThe New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on.\r\n\r\nThe network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.\r\n\r\nThe impersonation level field indicates the extent to which a process in the logon session can impersonate.\r\n\r\nThe authentication information fields provide detailed information about this specific logon request.\r\n\t- Logon GUID is a unique identifier that can be used to correlate this event with a KDC event.\r\n\t- Transited services indicate which intermediate services have participated in this logon request.\r\n\t- Package name indicates which sub-protocol was used among the NTLM protocols.\r\n\t- Key length indicates the length of the generated session key. This will be 0 if no session key was requested.",
  "S1": "S-1-0-0",
  "S2": "-",
  "S3": "-",
  "S4": "0x0",
  "S5": "S-1-5-21-1009658894-4016096118-1013530418-1275",
  "S6": "blacklisted.user1",
  "S7": "Demo",
  "S8": "0xc2c9fa762",
  "S9": "3",
  "S10": "NtLmSsp ",
  "S11": "NTLM",
  "S12": "RemoteWorkstation",
  "S13": "{00000000-0000-0000-0000-000000000000}",
  "S14": "-",
  "S15": "NTLM V1",
  "S16": "128",
  "S17": "0x0",
  "S18": "-",
  "S19": "10.10.10.10",
  "S20": "44214",
  "S21": "%%1833",
  "S150": ""
}
```


S1 to S150 are extended string fields commonly used to store extracted, meaningful information from events. This data can then be correlated in dashboards or used to define alerting conditions.

Example: A DTS object can evaluate against a dynamic or static list of blacklisted or unknown users. The **getter function** checks whether the current user appears in a specified list (e.g., blacklist or whitelist).

- **Case 1:** If the user exists in a blacklist, an alert can be triggered using the **RaiseAsAlert** function to signal unauthorized access.
- **Case 2:** The user is on a whitelist: no alert is generated; however, relevant data can still be parsed and stored if necessary.
- **Case 3:** If the user is not found in either list, the **setter** function can be used to automatically add the unknown user to a blacklist.

To allow a DTS object to process an event, the following three prerequisites must be met:

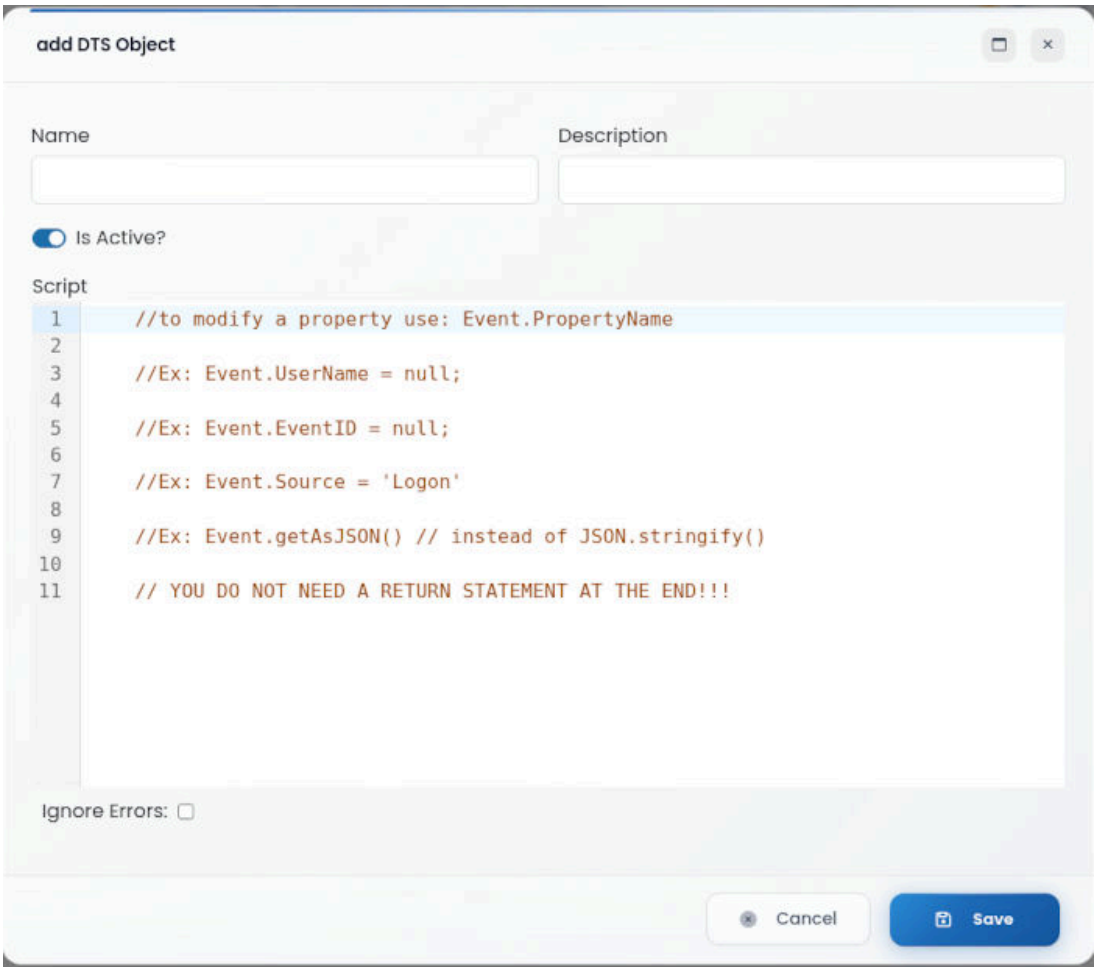
Create a **DTS object**

DTS Objects

A new DTS object can be created by navigating to the **Settings > Rules > DTS Objects** page. Use the **Add** button

Add DTS Object

on the page to define and create a new DTS object.



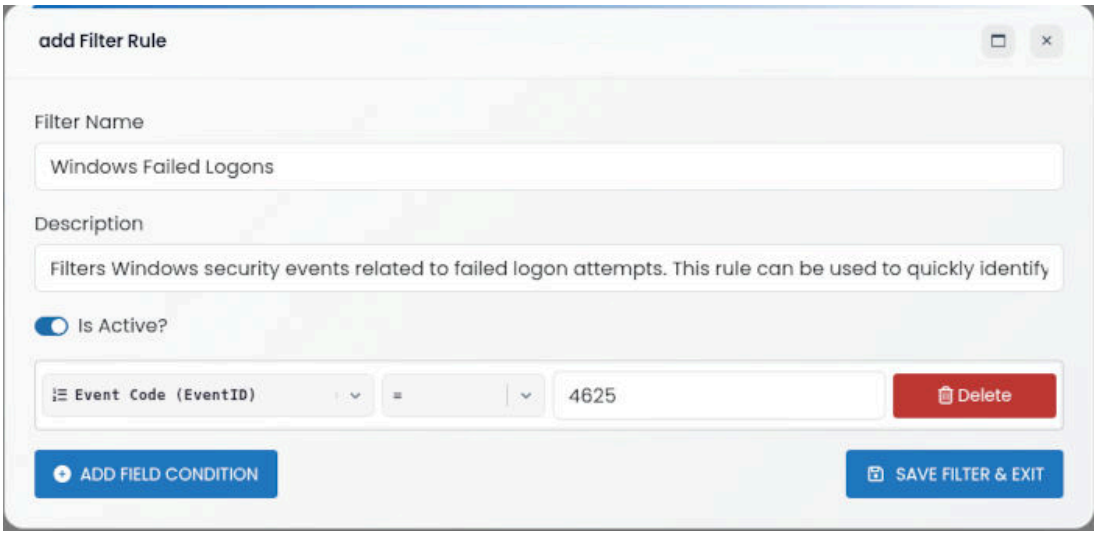
Create a **Filter rule**

A filter rule defines the conditions that incoming events must meet to be processed by one or more DTS Objects.

To create a new filter rule, navigate to **Settings > Rules > Filter Rules**. Use the ADD

Add Filter Rule

button on the page to configure and save the rule.



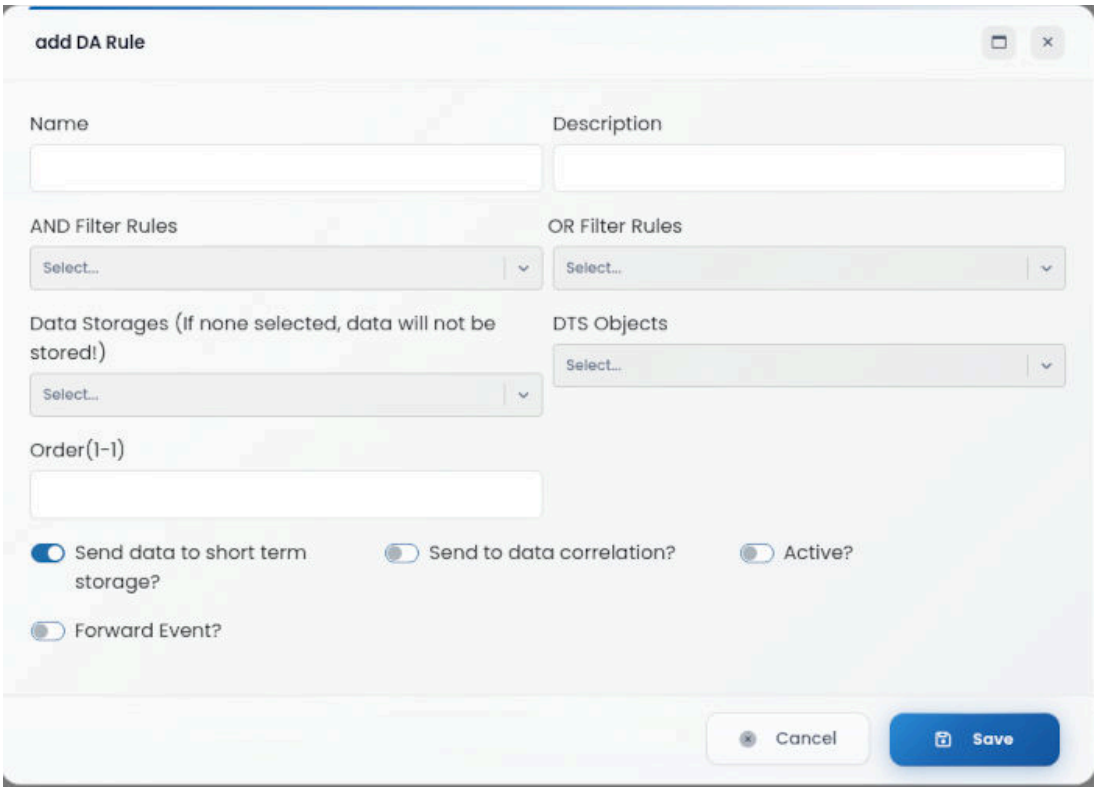
Create a **DA rule (data acquisition rule)**

A DA rule defines the decision-making process that routes events - filtered by previously defined Filter Rules - through DTS Objects and forwards them to the **Data Storage** and/or **Data Correlation** services.

To create a new DA rule, go to **Settings > Rules > DA Rules** and click the **Add**



button to configure and save the rule.



For more details on DTS objects, refer to the following section: DTS.

DTS Objects Built-in methods

DTS objects support built-in functions designed to interact with Redis lists and the alerting module. One of the available methods is:

1) `setter` function

Used to insert or update values in Redis lists.

Parameters: `[list_name],[list_key],[list_value][TTL]`

Example:

```
setter('UserLists', Event.UserName, Event.SrcIP, 360);
```

This example checks the `"UserLists"` Redis list for the value of the event's `UserName` field.

- **Case 1:** If the key (`UserName`) already exists, the function updates its value with `SrcIP` and resets the TTL (time to live) to 360 seconds.
- **Case 2:** If the key does not exist, a new entry is created with `UserName` as the key, `SrcIP` as the value, and a TTL of 360 seconds.

2) `getter` function

This function obtains values from Redis lists.

Parameters: `[list_name], [list_key]`

Example:

```
getter('IPLists', Event.SrcIP);
```

In this example, the DTS object queries the `IPLists` Redis list using the value of the event's `SrcIP` field as the key and returns the associated value, if present.

3) `RaiseAsAlert` function

This function triggers an alert event based on custom parameters.

Parameters: `[event_list] (JSON format)`, `[alert_name]`, `[email_address(es)]`, `[security_score]`, `[security_level]`, `[alert_template]`

Example:

```
RaiseAsAlert(Event.getAsJSON(), "MultipleLogins(10)", "someone@company.com", "7", "7", "Multiple Logins(10)");
```

In this example, the DTS object sends an alert named **"Multiple Logins (10)"** to **someone@company.com**, assigning it a **security score** of 7 and a **security level** of 7.

4) `backEvents` function

This function searches past events based on a specified string and returns matching results in JSON array format.

Example:

```
backEvents('SearchString', NumberOfDays, NumberOfEvents);
```

- **SearchString** – The query string used to filter historical events.
- **NumberOfDays** *(optional)* – Time window to look back; defaults to 100 days if not specified.
- **NumberOfEvents** – Maximum number of events to return.

5) `backCount` function

Returns the number of events that match a specified search query within a given time range.

Example:

```
backCount('SearchString', NumberOfDays);
```

SearchString – The term or condition used to filter past events.

NumberOfDays – The time range (in days) to look back when counting matching events.

6) `ConsoleLog` function

Writes the specified string to the acquisition log file.

Example:

```
ConsoleLog(String);
```

The message is logged to: */var/log/data-acquisition.log*

Alert scenarios

Alerts examples

Example 1. Create a Logon alert scenario example

This scenario demonstrates how to configure a real-time alert that triggers when a specific user experiences two failed logon attempts within a 60-second window.

Step 1:

Navigate to **Settings > Alerts > Realtime**.

Click **CREATE ALERT** to begin configuring the new alert.

Step 2:

Create an alert definition with the following parameters:

- **Name**: `Default - Audit policy change`
- **ALERT ACTIVE**: Active
- **Alert Security Score**: 40
- **Alert Security Level**: 5
- **Send as Alert**: Active

Step 3:

Add a new rule to the alert definition using the criteria below:

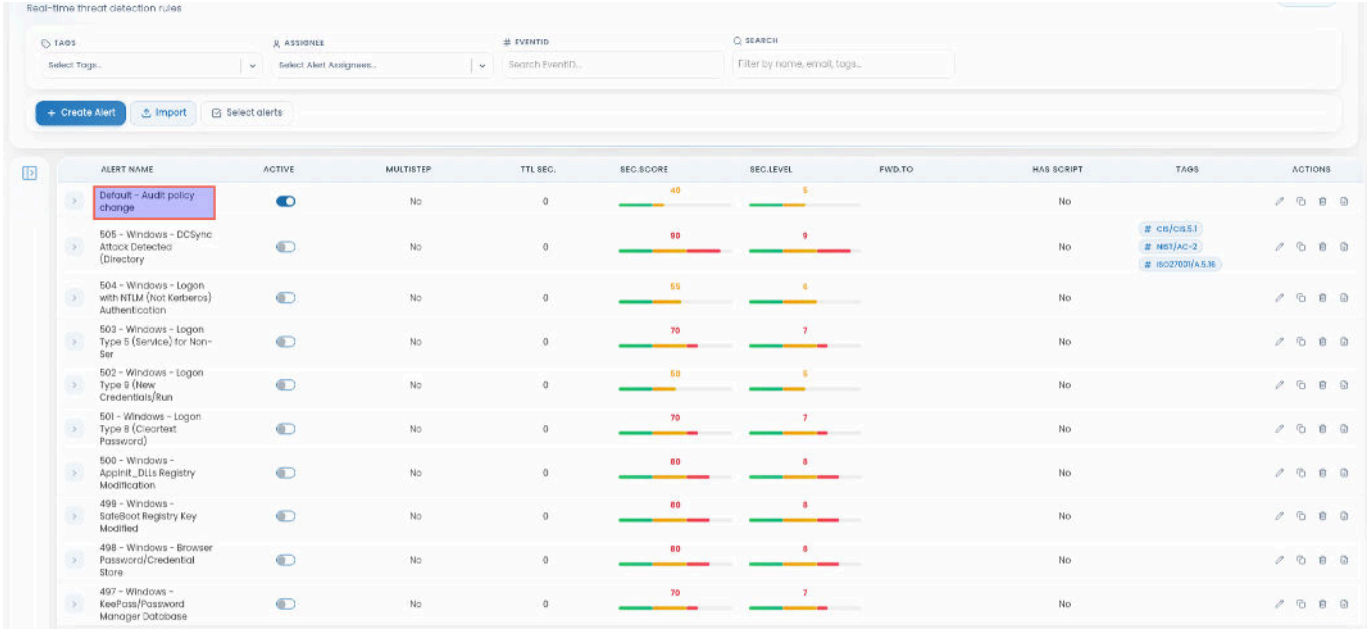
- **Description**: `Audit policy change events`
- **Event ID**: `4719`

  Event IDs can be referenced in the Event Dictionary

Step 4:

Save the alert definition. It will now appear in the **Alerts** list.

The new definition shows in **Alerts** page



Step 5:

Once configured, the system will generate alerts in real time whenever the defined conditions are met. In this example, the alert triggers upon detecting Windows Event ID `4719` (Audit Policy Change) from the Windows Security Log.

Example 2. Configuring a Logon summary alert scenario example

This scenario sets up an alert to notify the security officer when a user fails to authenticate more than 50 times within a single day.

Step 1:

Create a report that defines the alert conditions - for example, events where authentication fails (EventID 4625: *An account failed to log on*). This report identifies matching events and can be configured to send notifications containing key details like the network address, username, date, time etc.

- Open the **Browser** module
- Search for `EventID:4625` (Windows event ID for failed logon)
- Click **Filter data** to display relevant events
- Click **Save** and select **Save as New Report**
- Enter a name and description such as *An account failed to log on*
- By default, the report will be saved under **Custom Reports** in the **Reports** module

Step 2:

Create a new summary alert using the previously saved report:

- Navigate to **Settings > Alerts > Summary**
- Click **ADD REGISTERED SUMMARY ALERT**
- Configure the summary alert with the following settings:
  - Report: the saved custom report
  - Security Score: 50
  - Security Level: 5
  - SummaryOn Level 1: `UserName`
  - SummaryOn Level 2: `Computer`

Step 3:

Monitor the results to verify that alerts are triggered when the threshold is exceeded.

Example 3. Distributed Denial of Service (DDoS)

Alert description

This alert is designed to trigger when 100 or more communication events are directed to the same IP address and port within one minute, originating from different source IPs. The scenario identifies potential Distributed Denial of Service (DDoS) attempts.

Required Data Sources

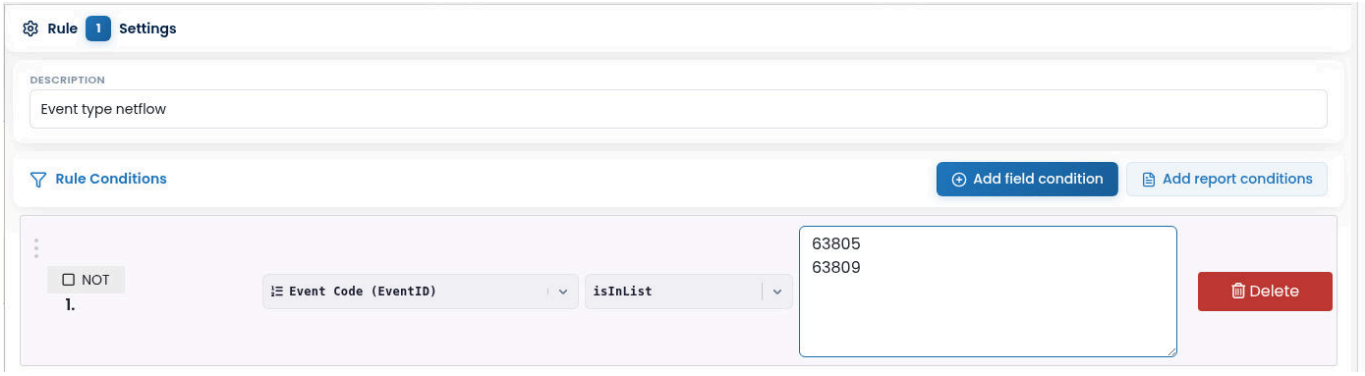
- **Firewall NetFlow events** must be collected and available in CYBERQUEST for this alert to function correctly.

Alert setup

From the **Settings** menu, navigate to **Alerts > Realtime**.

1)**Rule 1 - Identify NetFlow Events**

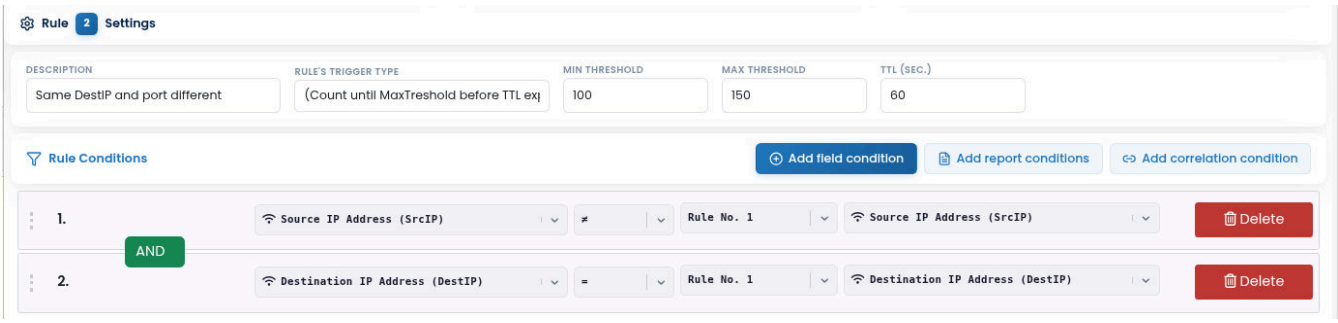
- **EventID**: `63805, 63809`
- Use the **isinList** operator to detect events with the specified IDs.



2)**Rule 2 - Set DDoS Detection Criteria**

In the Rule 2 section, configure the following:

- **Min Threshold**: `100`
- **Max Threshold**: `150`
- **TTL**: `60` seconds
- **SrcIP** ≠ Rule No. 1 **SrcIP**
- **AND**
- **DestIP** = Rule No. 1 **DestIP**



To export the alert settings as a CQO configuration file, use the following link: **Alert Object**

Example 4. Application credentials sharing

Alert description

Detects a scenario where a Windows logon is followed by an application logon from the same IP address but with a different user account - indicating potential credential sharing.

Required Data Sources

To configure this alert, the following data sources must be collected in CYBERQUEST:

- Windows Security Log with Logon auditing enabled via Group Policy (GPO)
- Application logon audits that include both username and source IP address

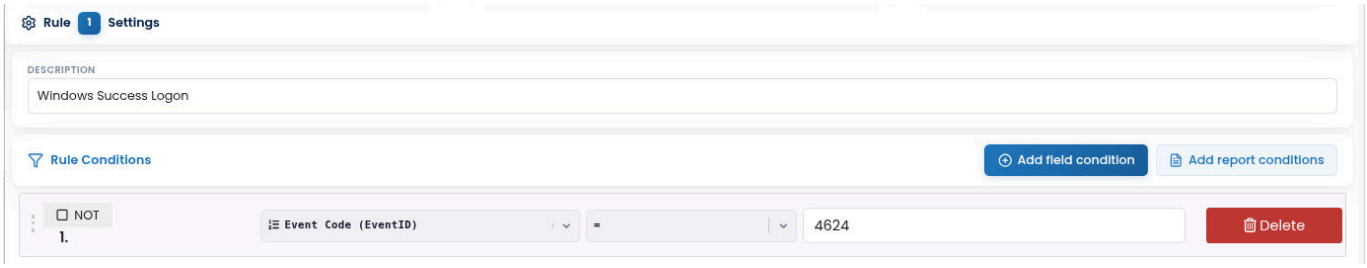
Alert setup

Navigate to **Settings > Alerts > Realtime**.

1)**Rule 1 - Windows Logon Event**

Identify Windows Success Logon events using Event ID 4624. Configure as follows:

- **EventID** = `4624`

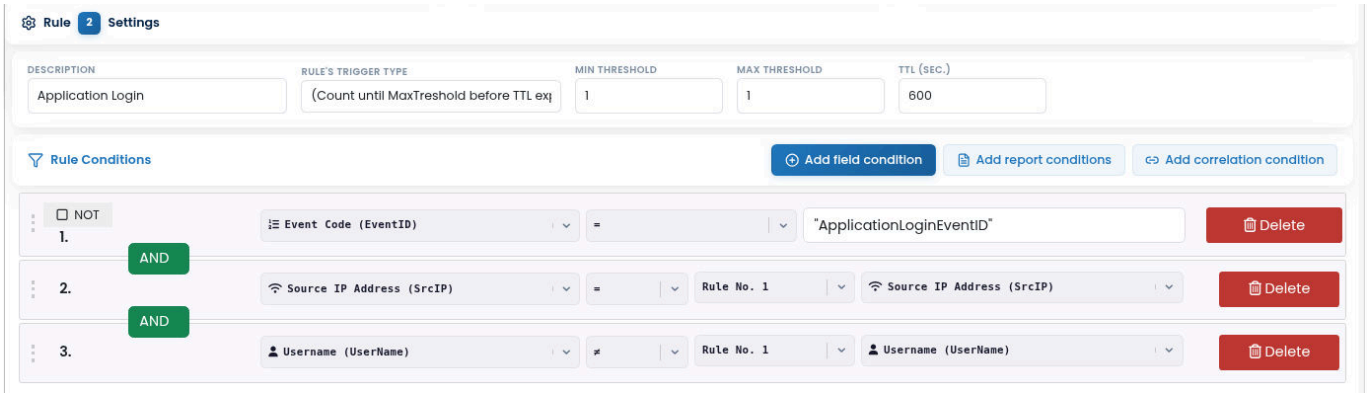


2)**Rule 2 - Application Logon Event**

Capture application login activity with different credentials from the same source IP:

To do that:

- **EventID** = `ApplicationLoginEventID`
- AND
- **SrcIP** = Rule No. 1 **SrcIP**
- AND
- **UserName** ≠ Rule No. 1 **UserName**



To export the alert configuration as a `.cqo` file, use this link: **Alert Object**.

Example 5. Malicious IP or domain

Alert description

This alert triggers when communications occur between internal IP addresses and those listed in a blacklist containing known malicious IPs and domains.

Required Data Sources

To enable this alert, the following data must be collected in CYBERQUEST:

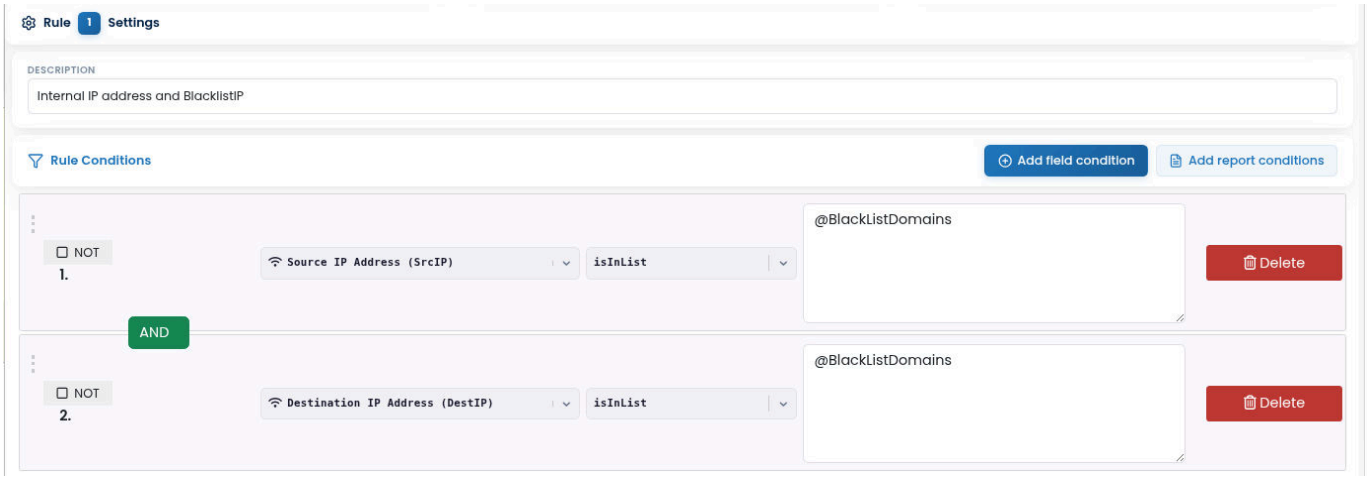
- Network communication events;
- Blacklist and/or security feeds.

Alert Configuration

Navigate to **Settings > Alerts > Realtime**.

In Rule 1, enter the following settings:

- **SrcIP isinList @BlackListDomains**
- **AND**
- **DestIP isinList @BlackListDomains**



To export the alert configuration as a CQO format file, use the following link: **Alert Object**.

Example 6. Successful login after multiple attempts

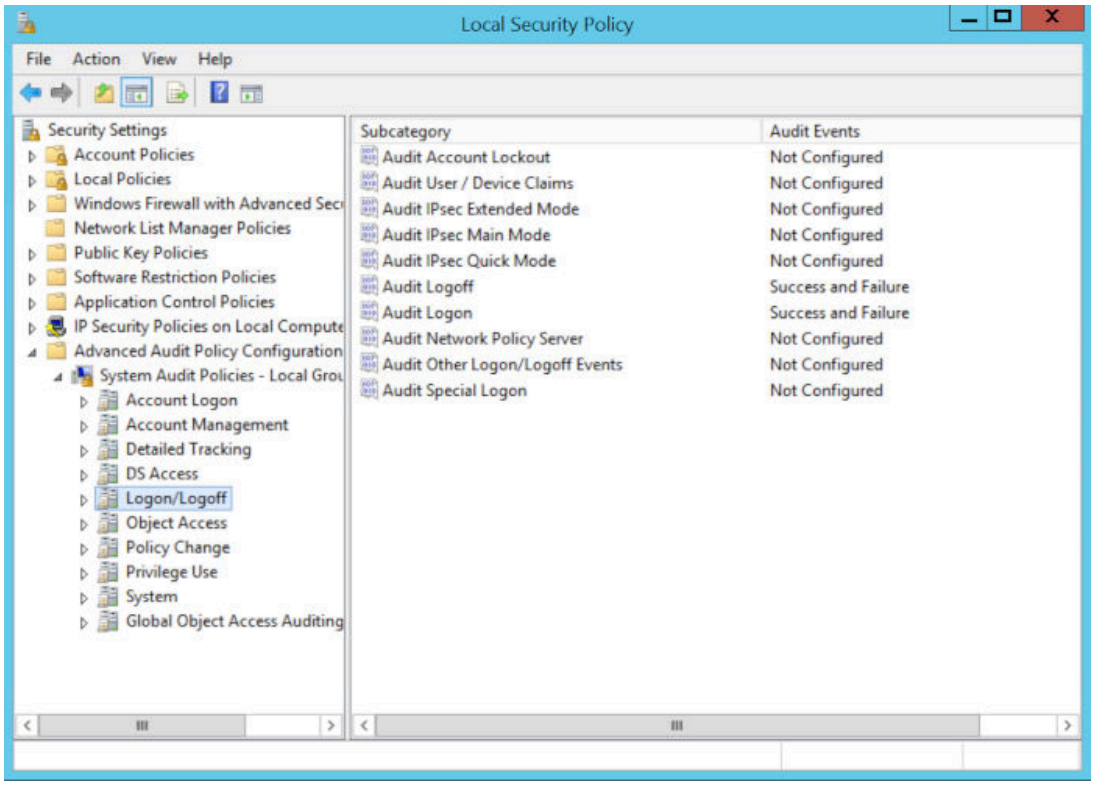
Alert description

Triggers an alert when a user successfully logs in after at least five failed attempts within a 10-minute window.

Data Sources Required

To enable this alert, ensure the following data source is being collected in CYBERQUEST:

- Windows Security Log with Logon auditing enabled via Group Policy.



Alert Setup

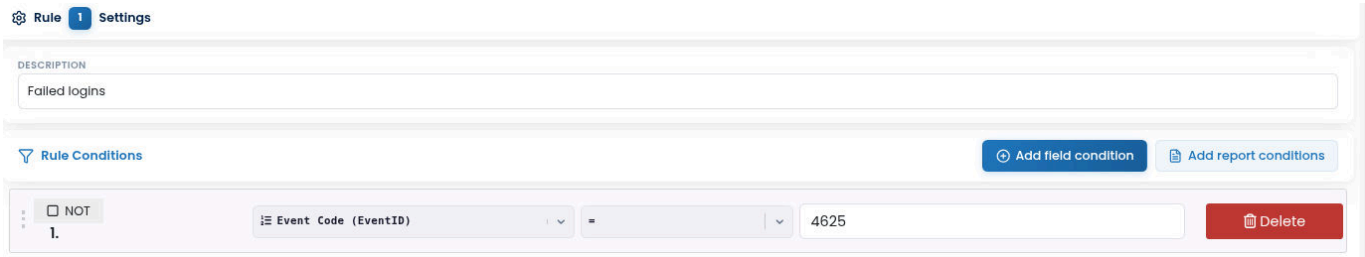
- Open the CYBERQUEST Web Interface.
- Navigate to **Settings** > **Alerts** > **Realtime**.
- Create a new alert by clicking the

  button.
- Add the **first rule** to detect Windows Failed Logon events by clicking

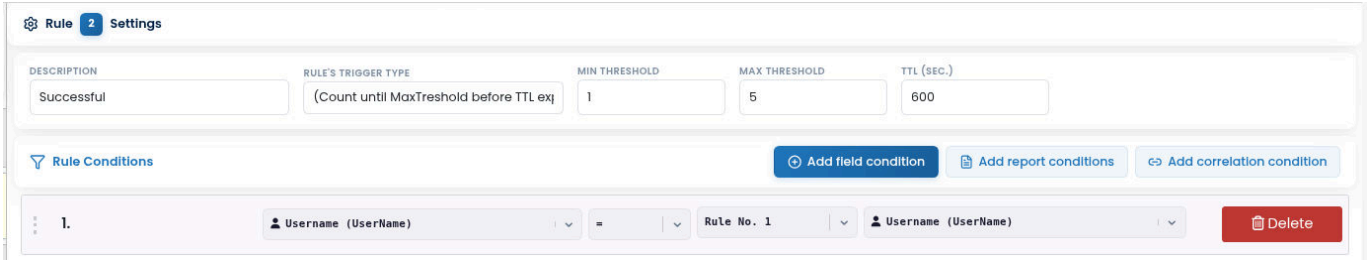
  

  and setting **EventID = 4625**.

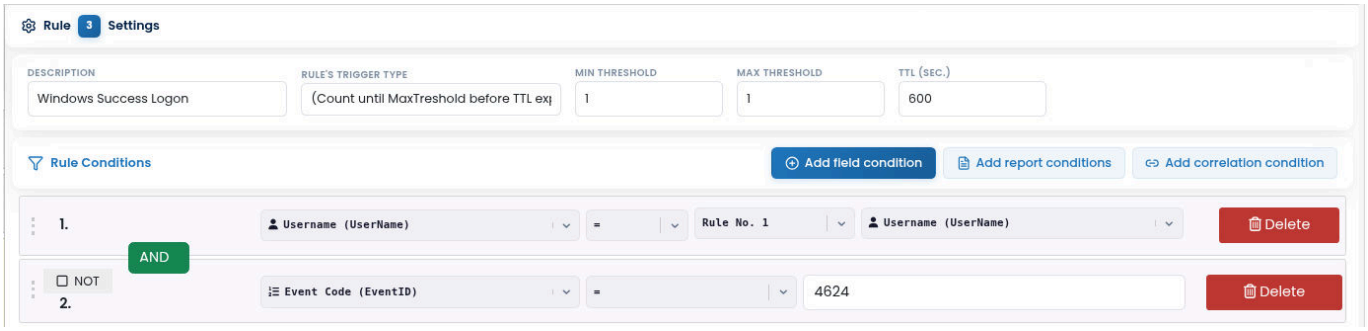


- Add the **second rule** by clicking

  , and configure **UserName = Rule No. 1 UserName**.



- Add the **third rule** with a correlated condition:
  - **UserName = Rule No. 1 UserName**
  - **EventID = 4624** (successful logon)



- Click the

  button at the top-left to save the alert configuration.

To export this alert setup in CQO format, use the following link: **Alert Object**.

Example 7. Traffic to infected domains

Alert Purpose

This alert is triggered when access to malicious domains listed in `@BlackListDomains` is detected.

Data Sources Needed

- **Web access events**

Description

- Open the CYBERQUEST Web Interface.

Navigate to **Settings** > **Alerts** > **Realtime**.

Click the

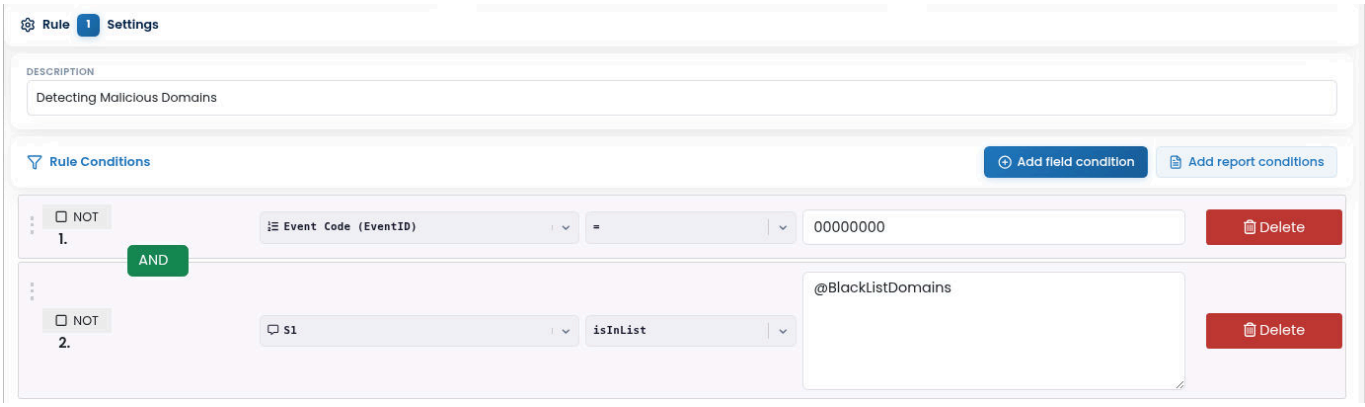


button to create a new alert.

- **Rule 1** – Configure the condition as follows:

```
EventID = [Event ID for web access events]
```

```
Accessed domain field isinList @BlackListDomains
```



To export this alert setup in CQO format, use the following link: **Alert Object**.

Example 8. VPN Login and RDP with different users

Alert Purpose

This alert is triggered when a VPN login is followed by an RDP connection from the same host but using a different user account than the one used for the VPN session.

Required Data Sources

- **VPN login events**
- **Windows Security Log**

Configuration Steps

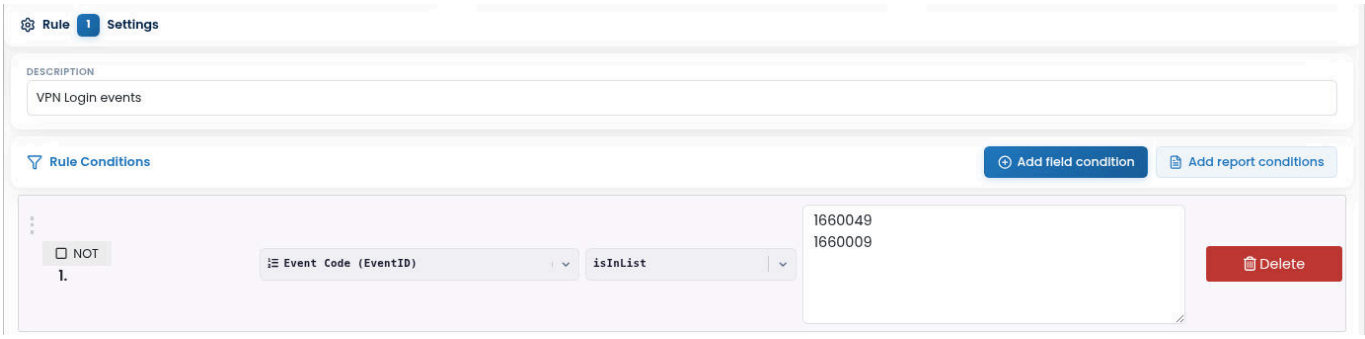
- Open CYBERUEST Web Interface.
- Navigate to **Settings** > **Alerts** > **Realtime**.
- Click the

  button to create a new alert.

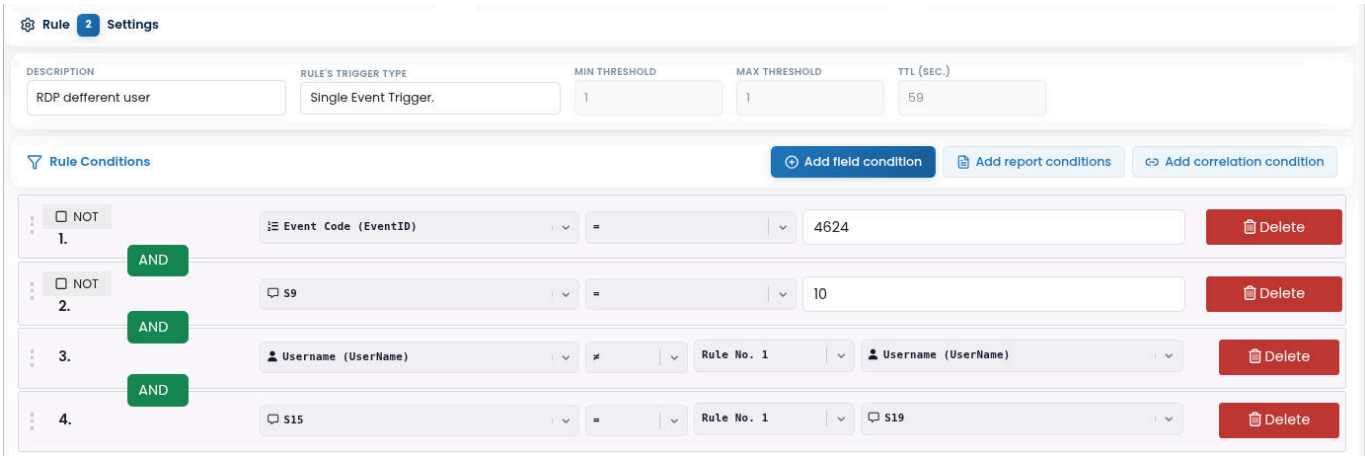
1)**Rule 1** – Detect VPN login events:

- `EventID isinList 1660049, 1660009`



2)**Rule 2** – Detect RDP login from the same host using a different user:

- `EventID = 4624`
- `S9 = 10`
- `UserName ≠ Rule No. 1 UserName`
- `S15 = Rule No. 1 S19`



To export this alert setup in CQO format, use the following link: **Alert Object**.

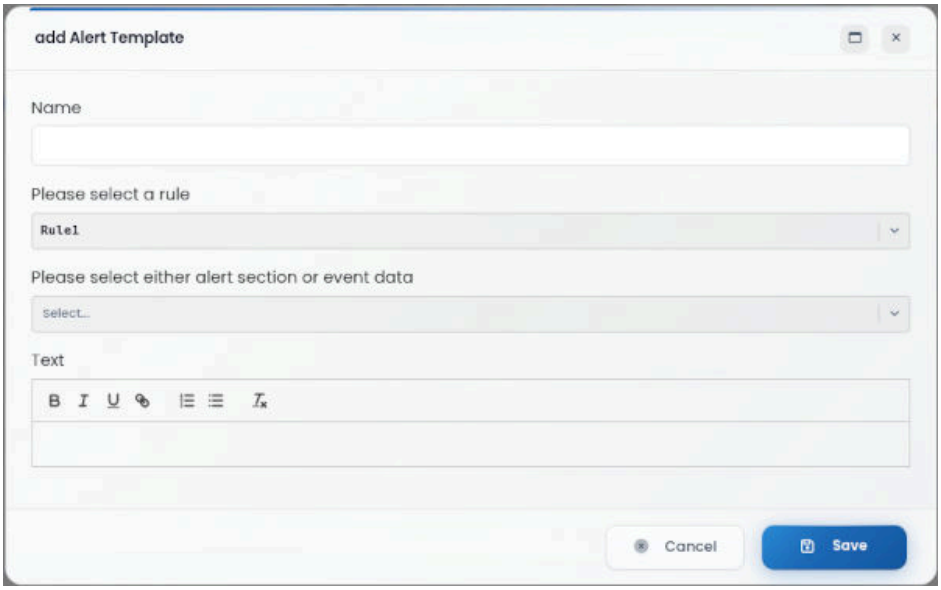
Notification templates customization

From the **Settings** menu, navigate to **Alerts > Notification templates**. This opens the **Alert Templates** section of the Alerts customization interface.

The **Actions** menu allows editing or deleting existing alert templates. The **Alert Templates** page lists all defined templates and includes an option to create a new one.



To create a new alert template, select the *NEW ALERT TEMPLATE* option from any of the pages mentioned above. This opens the *NEW ALERT TEMPLATE* page. The available settings are similar to those in the **Edit Alert Template** page, accessible from the **Alert Templates** list.



- In the **Name** field, enter a unique name for the alert template.
- From the **Please select a rule** drop-down list, choose the rule (e.g., *Rule1*, *Rule2*, *Rule3*, or *Rule4*) that the template will reference.

- In the **Please select either alert section or event data** field, specify whether to use an alert section or event data as the source.
- In the **Text** field, enter a descriptive message or insert dynamic objects as needed.

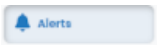
Click the "***Save***" button to save the changes and return to the **Alert Templates** page.

Viewing Alerts

Working with Alerts Module

The **Alerts** module in CYBERQUEST provides real-time visibility into security incidents and policy violations. It allows users to monitor, filter, and investigate alert events generated based on predefined rules and thresholds. This section outlines how to navigate the Alerts interface, apply filters, and interpret results to support security operations and incident response.

Access the **Alerts** module by clicking the



button located on the left-hand panel of the Web Interface.

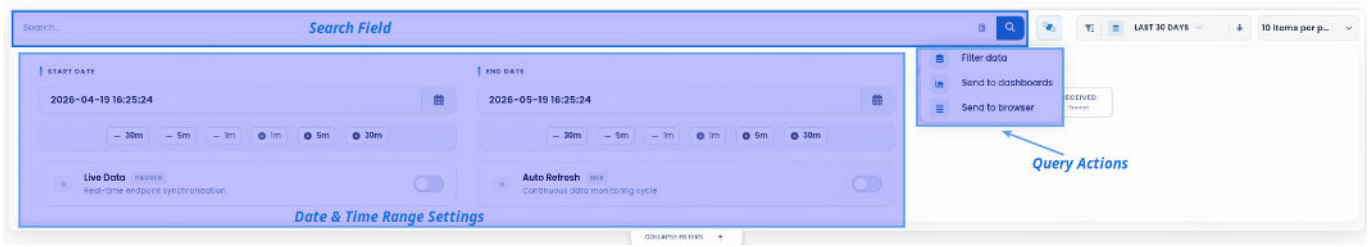
The module is divided into two main sections:

- **Search and Filter** - Enables precise control over the alert data displayed.
- **Results** - Displays alert records based on the selected filters and search criteria.

Alerts Search and Filter section

This section provides control over which alerts are shown in the results list. To access it, expand the filters by clicking the

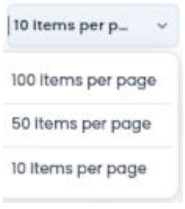
button. Once expanded, the filtering options become available.



The **Search field** allows filtering of displayed alerts using free-text input. If left empty, all available events are shown.

A detailed guide on using free-text search is included in this manual.

To control how many alerts are shown per page, press the



button. The default is 10 items, but options for 50 or 100 are also available.

Other options in the **Search and Filter** section:

- **Filter data** - Applies the selected filters and updates the alert results list accordingly.
- **Send to Dashboards** - Opens the filtered results in the **Dashboards** module in a new browser tab.
- **Send to Browser** - Opens the filtered results in the **Browser** module in a new browser tab.

The **Search and Filter** section offers options to specify the date and time range for the displayed information. This is especially useful for quickly reviewing compliance within a chosen period.

Users can set a custom start and end date or select from predefined intervals like last hour, day, two days, three days, ten days, 30 days, or 90 days. By default, the **Alerts** interface shows all alerts. Convenient buttons below the **Start Date** and **End Date** fields allow adjusting the time range and choosing the time reference, including GMT, Local Time, Received Time, Now, or enabling AutoRefresh.



GMT - Converts the selected time range to Greenwich Mean Time.

LocalTime - Refers to the local system time when the event actually occurred.

ReceivedTime - Indicates the moment the event was received by the CYBERQUEST system.

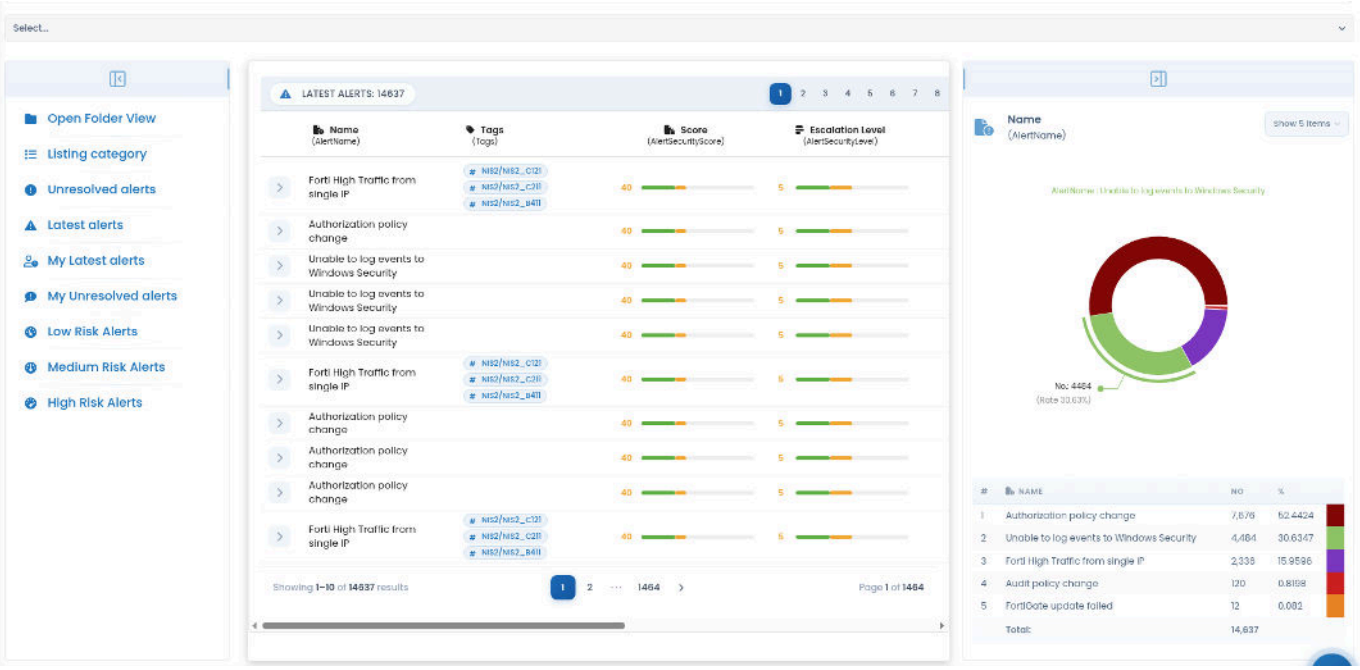
Now - Automatically updates the end time to the current moment.

Live Data - Keeps the time range synchronized with the current time, continuously updating the displayed date/time window without automatically refreshing the event results.

AutoRefresh - Periodically refreshes the results using the current time window, displaying the latest alerts according to the configured refresh interval.

Alerts Results section

This section is the main area where triggered alerts are displayed. Alerts appear in chronological order, and the number of entries per page depends on the settings defined in the Search and Filter section. Multiple viewing formats are available for reviewing alert data:

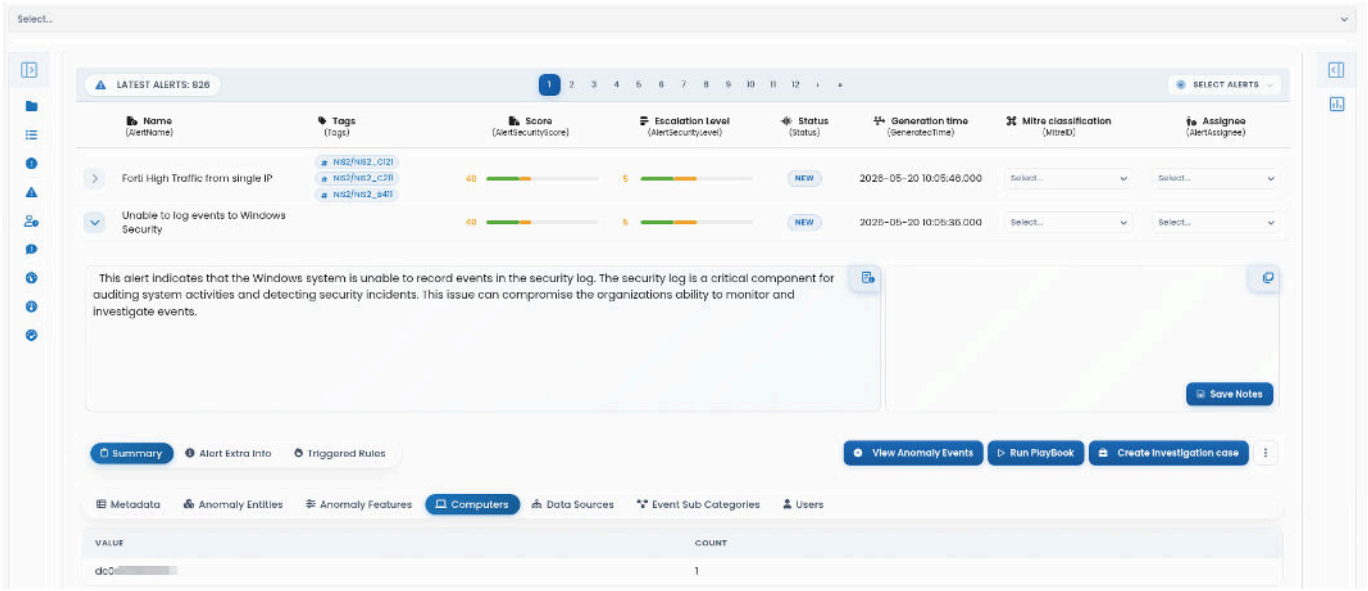


- *Open Folder View* - Opens the folder-based navigation view, allowing users to browse alerts by folders or categories.
- *Listing category* - Displays the current classification of alerts based on the stage of the attack lifecycle or operational focus (e.g., tactics like as initial access, lateral movement, or data exfiltration).
- *Unresolved Alerts* - Displays all active alerts that have not yet been addressed or closed, requiring a status change to mark them as resolved.

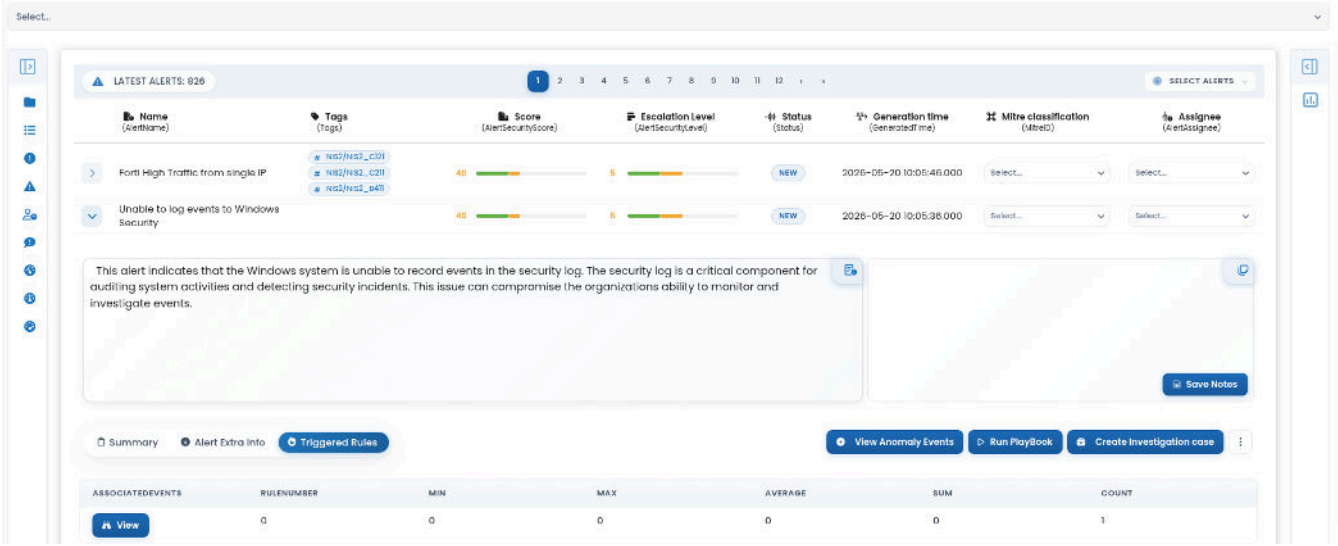
- *Latest Alerts* - Displays the most recently generated alerts.
- *My Latest Alerts* - Shows the latest alerts that are specifically assigned to or created by the currently logged-in user.
- *My Unresolved Alerts* - Displays all unresolved alerts that are assigned to the current user, helping prioritize personal alert triage.
- *Low Risk Alerts* - Alerts that indicate low severity or impact, typically informational or minor issues that require minimal action.
- *Medium Risk Alerts* - Alerts representing moderate risk or impact that may require attention but are not immediately critical.
- *High Risk Alerts* - High-severity alerts indicating serious risks, threats, or failures that require urgent investigation and action.

Detailed functionalities of the **Alerts** page are covered under the *Real-Time Alerts Customization* section.

Clicking an alert name in the **Alert Name** column opens the **Alert Viewer** pop-up, where detailed information about the triggered alert. The following elements are particularly relevant for investigation:



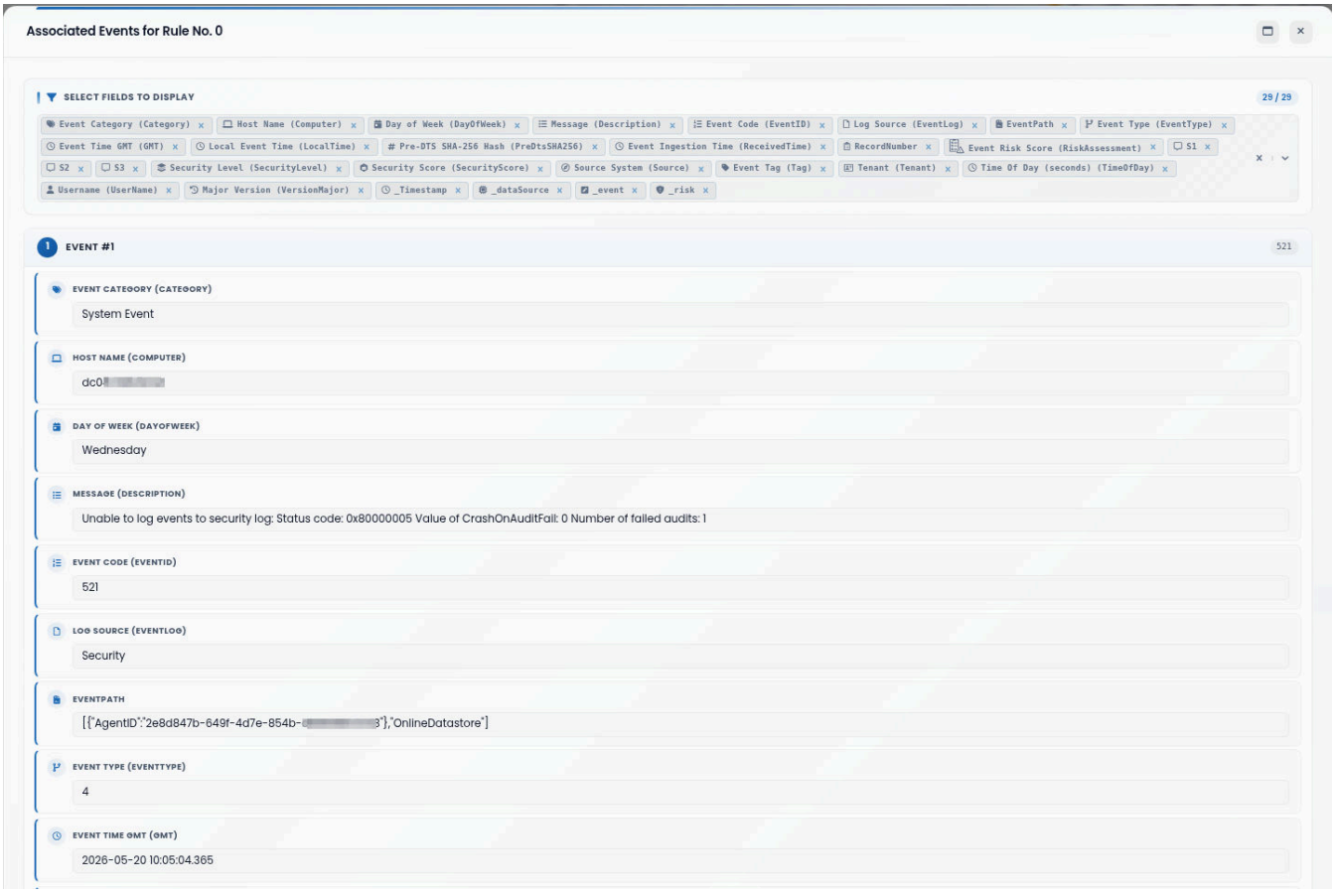
- **AlertSecurityLevel** refers to the current security level of the triggered alert, calculated based on the baseline defined in the alert definition.
- **AlertSecurityScore** indicates the current security score of the triggered alert, also derived from the baseline specified in the alert definition.
- The **Assets** tab displays all assets associated with the triggered alert.
- The **Computers** tab displays all computers currently impacted by the alert.
- The **DataSources** tab lists the data sources that contributed to generating the alert.
- The **EventSubCategories** tab shows the event subcategories linked to this alert.
- In **Users** tab are listed all users currently affected by this alert.
- Selecting **Alert Extra Info** displays the unique alert ID along with the correlation index used to trigger the alert and compute its security level and score.
- Selecting **Triggered Rules** shows a brief report outlining which rules from the alert definition were activated.



- Clicking the



button next to an entry opens a full report showing the events linked to that specific triggered rule.





Security Alerts and Events Analytics and Reporting

Alerts Reports

The **Alerts Reports** functionality is available from the **Alerts** module by selecting the **Reports** button.

Reports are generated for the active analysis scope. The report window displays:

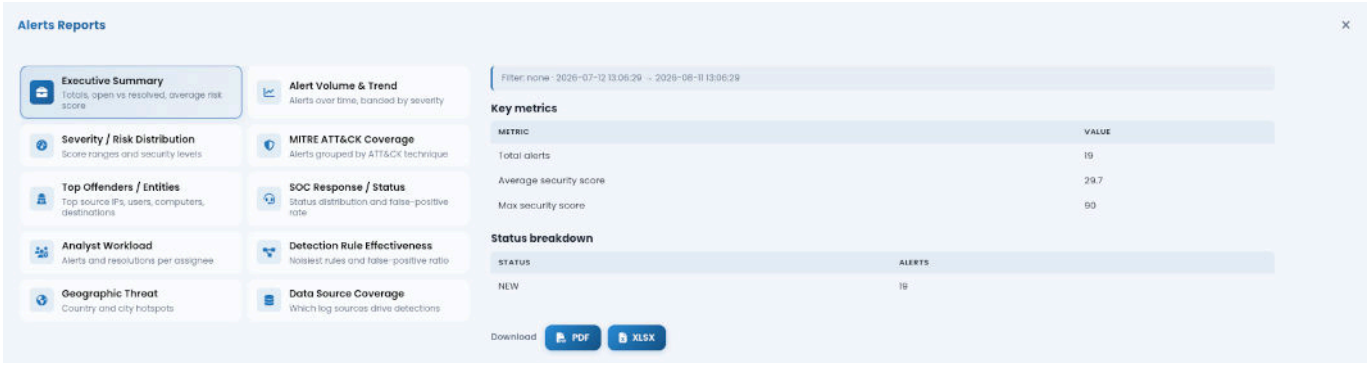
- the applied alert filter;
- the start and end of the reporting period;
- the report-specific metrics and aggregated results.

When no additional filter is applied, the report scope is displayed as **Filter: none**.

The following predefined reports are available.

Executive Summary

The **Executive Summary** report provides a high-level overview of the alerts generated during the selected period.



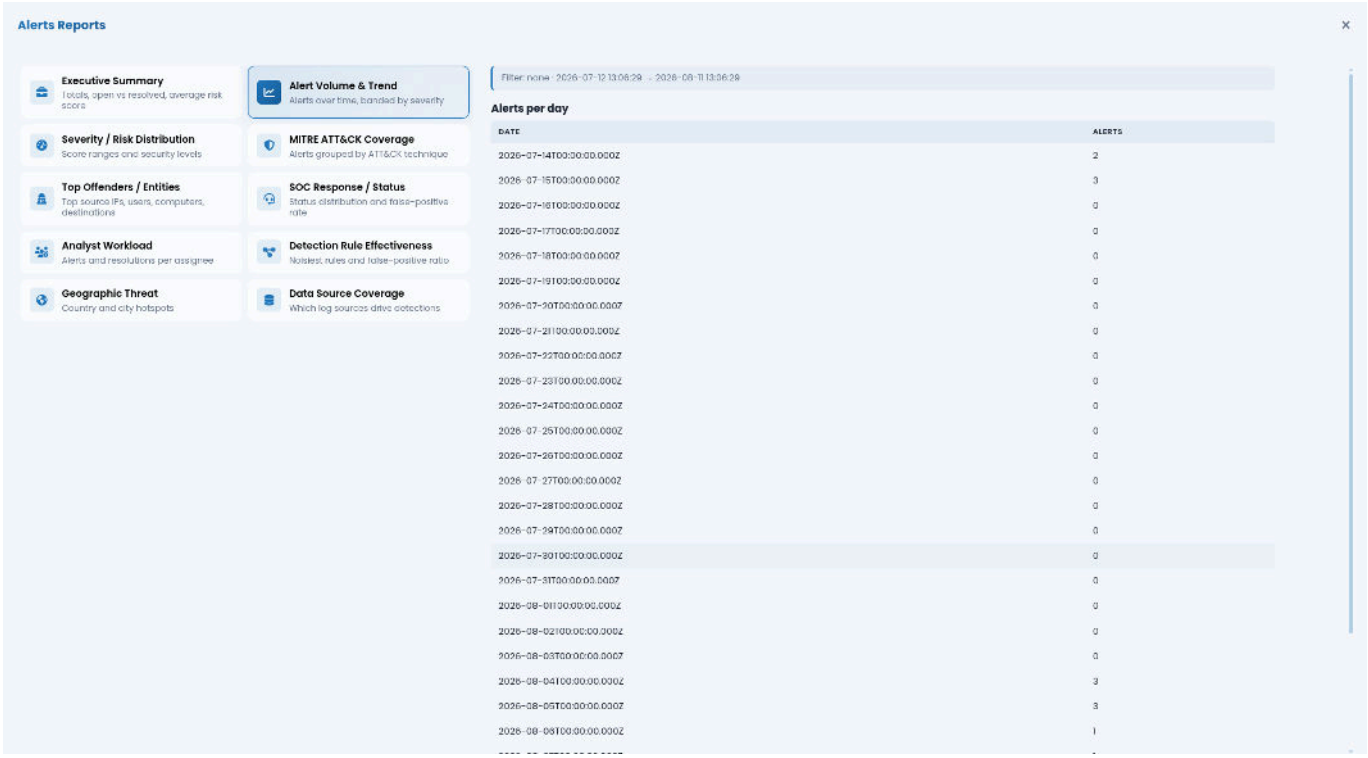
It includes:

- total number of alerts;
- average security score;
- maximum security score;
- distribution of alerts by status.

This report is intended for management-level review and for obtaining a concise assessment of the current alert landscape.

Alert Volume & Trend

The **Alert Volume & Trend** report presents the number of alerts generated for each day in the selected period.



It enables users to:

- analyze alert volume over time;
- identify increases or decreases in security activity;
- detect periods with unusually high alert generation;
- compare daily alert activity within the selected range.

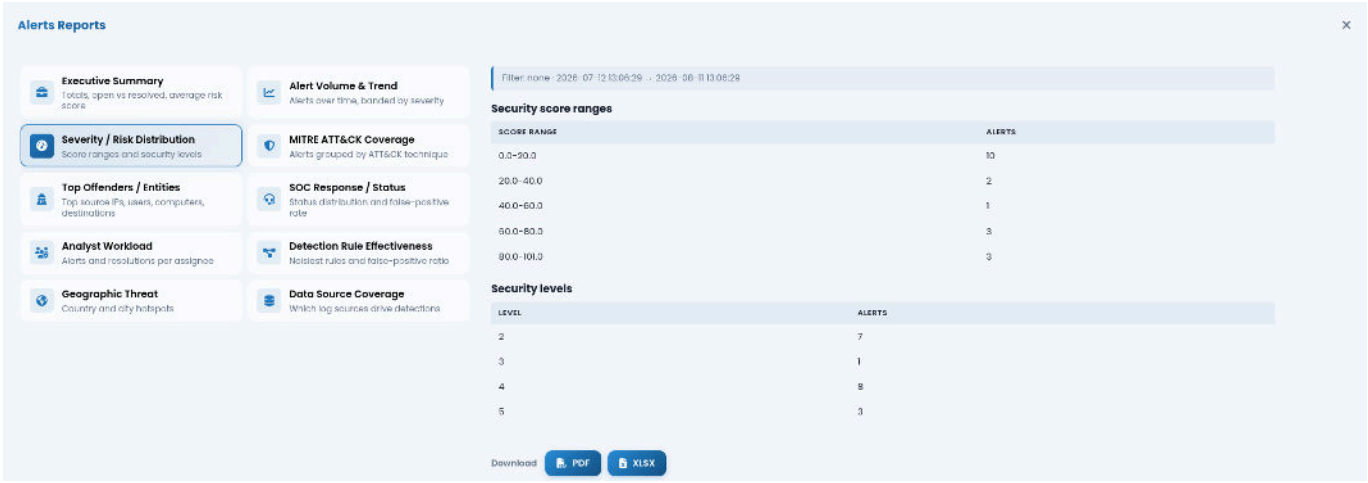
This report supports security trend analysis and operational monitoring.

Severity / Risk Distribution

The **Severity / Risk Distribution** report groups alerts according to:

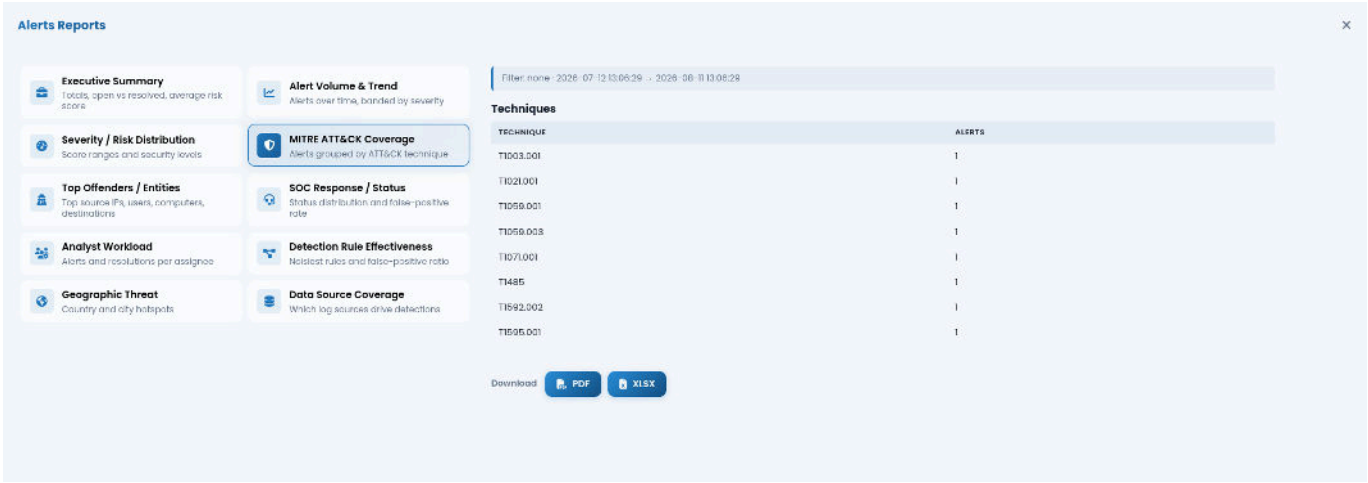
- security score ranges;
- security levels.

The report enables users to understand the risk profile of the generated alerts and to identify the number of alerts requiring higher investigation priority.



MITRE ATT&CK Coverage

The **MITRE ATT&CK Coverage** report groups alerts by the MITRE ATT&CK techniques associated with the detected activity.



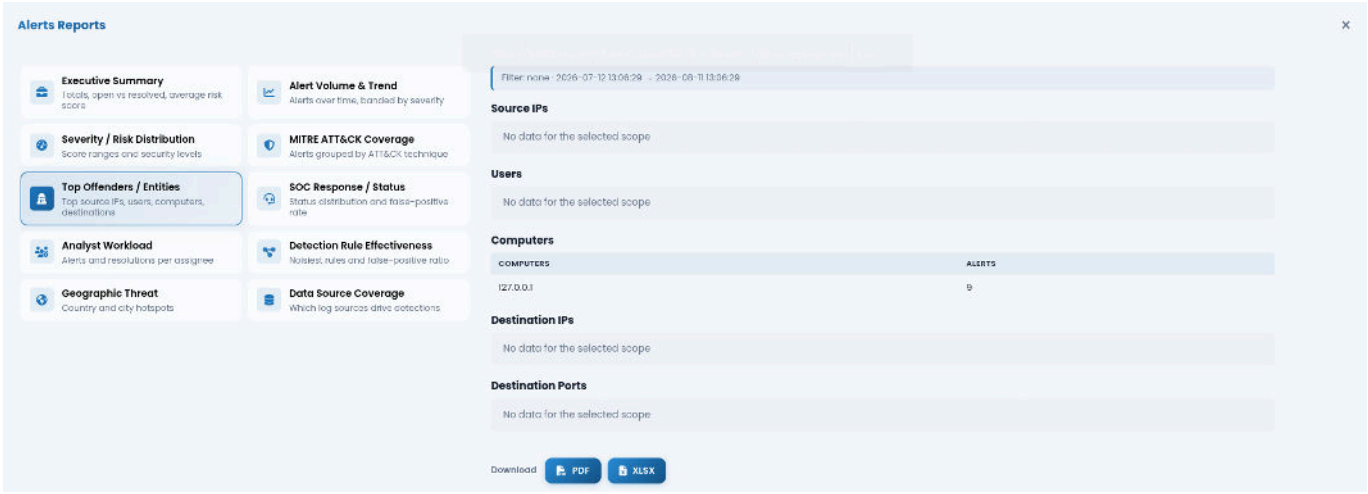
The report displays:

- the MITRE ATT&CK technique identifier;
- the number of alerts mapped to each technique.

This information allows users to assess which adversary techniques are being detected and to review the coverage of the organization's security monitoring controls.

Top Offenders / Entities

The **Top Offenders / Entities** report identifies the entities most frequently associated with security alerts.



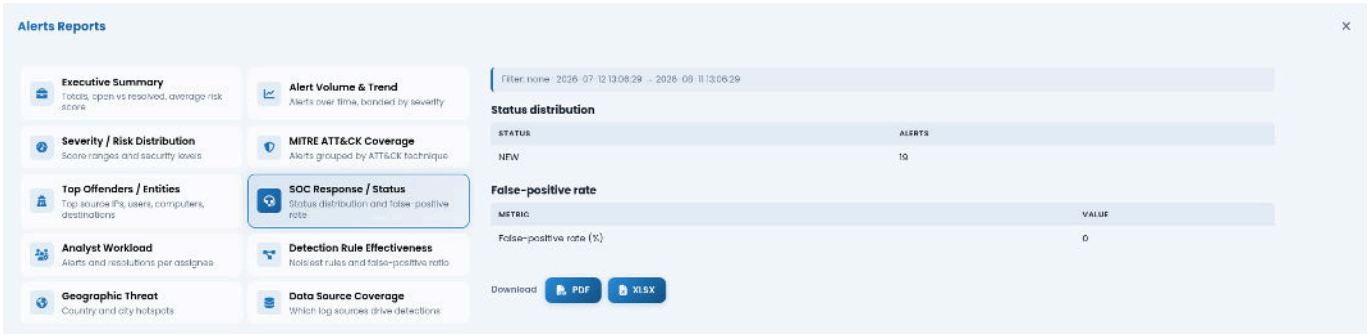
Depending on the information available in the alerts, the report can include:

- source IP addresses;
- users;
- computers;
- destination IP addresses;
- destination ports.

This report supports the identification of assets, accounts, or network entities repeatedly involved in suspicious activity.

SOC Response / Status

The **SOC Response / Status** report provides information about alert handling and classification.



It includes:

- alert distribution by status;
- false-positive rate.

The report can be used to monitor the current state of alerts and evaluate the quality of alert review and classification activities.

Analyst Workload

The **Analyst Workload** report presents alerts and resolutions grouped by the assigned analyst.



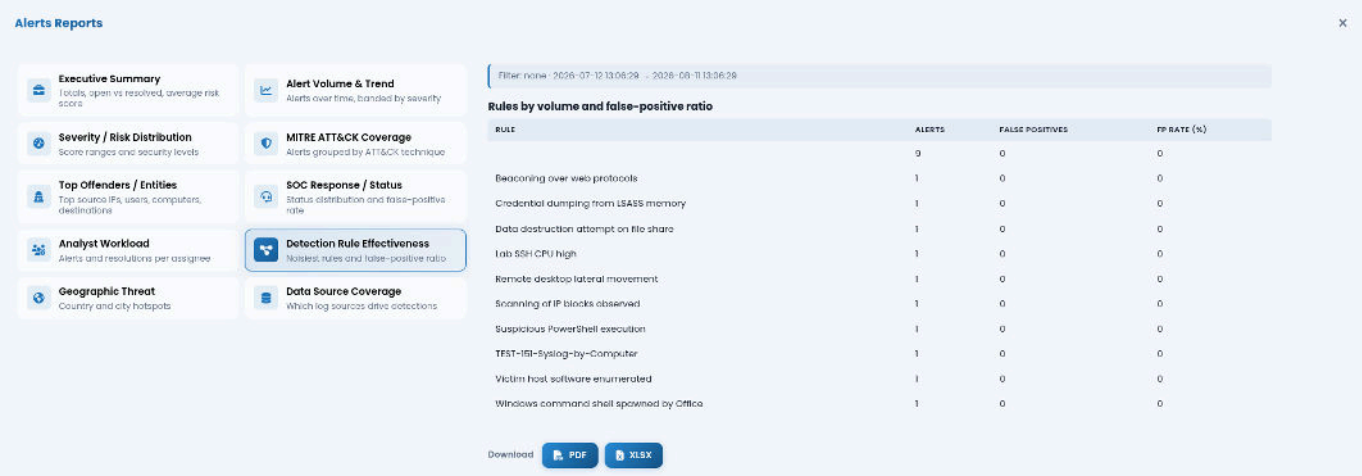
It supports:

- workload assessment;
- comparison of alert assignments;
- monitoring of analyst activity;
- identification of unassigned alerts.

Data is displayed only when alerts have been assigned to analysts within the selected reporting scope.

Detection Rule Effectiveness

The **Detection Rule Effectiveness** report evaluates the rules that generated alerts during the selected period.



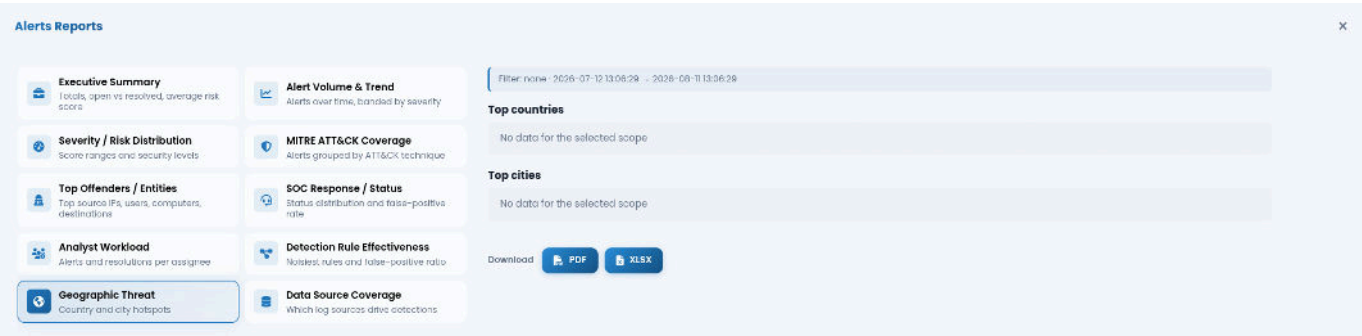
For each detection rule, the report can display:

- number of generated alerts;
- number of alerts classified as false positives;
- false-positive rate.

This report assists security teams in identifying frequently triggered rules, noisy detections, and rules that may require tuning.

Geographic Threat

The **Geographic Threat** report identifies geographic locations associated with security activity.



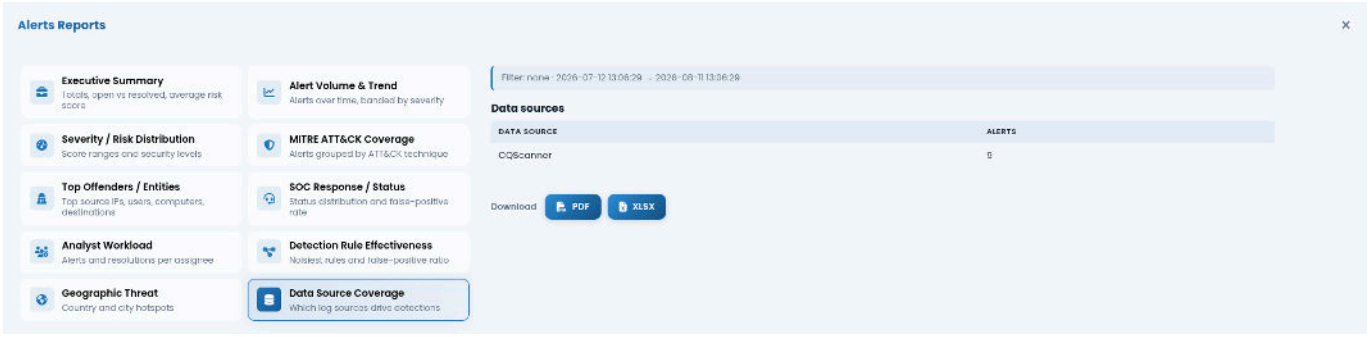
Where geographic information is available, the report includes:

- top countries;
- top cities.

The report supports the identification of geographic hotspots and potentially unusual sources of activity.

Data Source Coverage

The **Data Source Coverage** report identifies the data sources that contributed to alert generation.



It displays:

- data source name;
- number of associated alerts.

This report helps users determine which monitored technologies and log sources are contributing to security detections.

Report Export

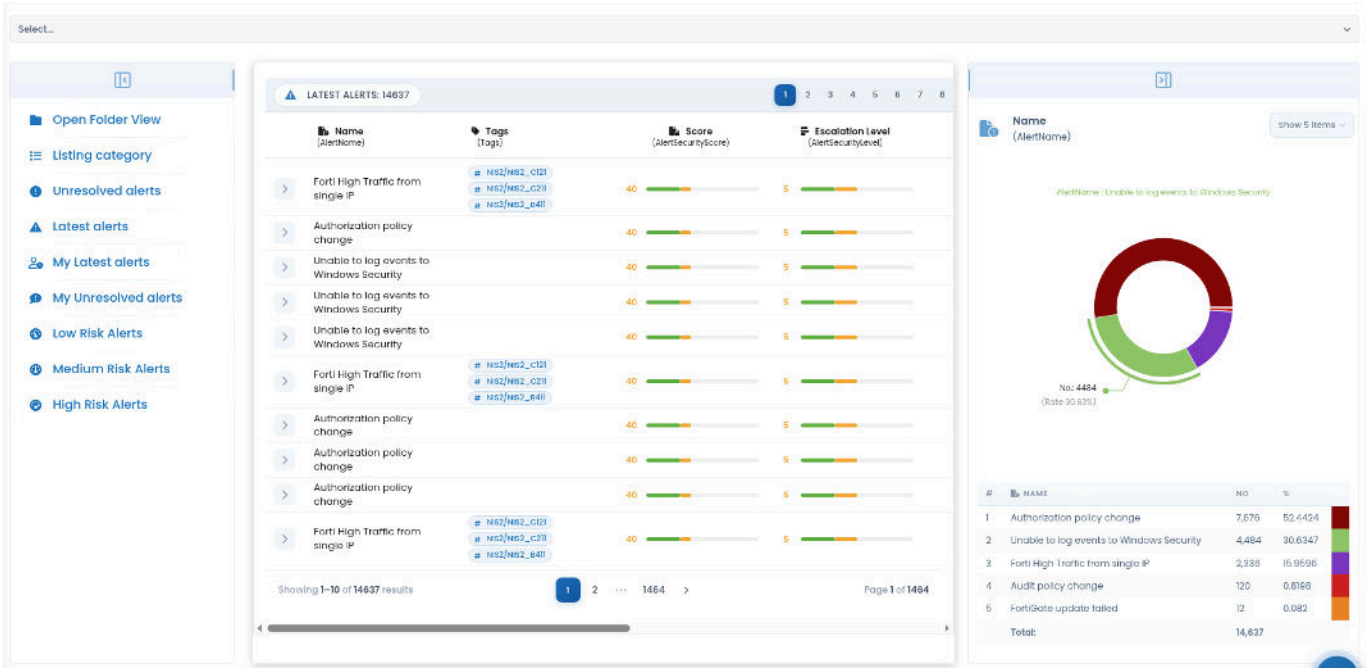
Each alert report can be downloaded in the following formats:

- **PDF**, for presentation, distribution, and archival purposes;
- **XLSX**, for additional analysis, filtering, and data processing.

The exported report contains the reporting period, the applied filter, and the metrics or aggregated results corresponding to the selected report type.

View triggered alerts

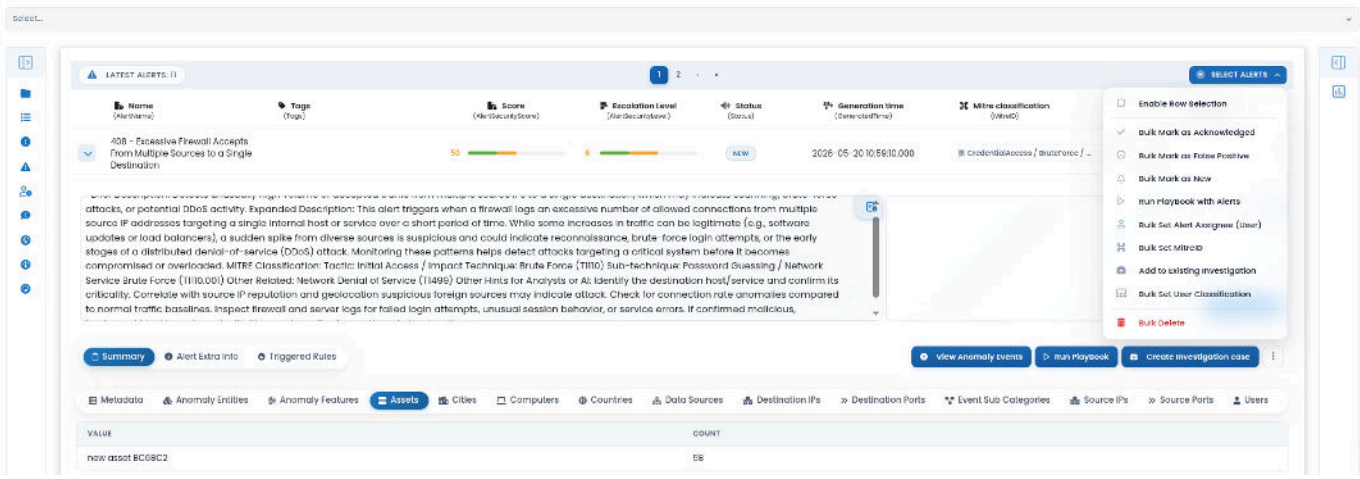
This area displays all triggered alerts in chronological order. The number of alerts shown per page depends on the settings configured in the **Search and Filter** section.



Clicking the



icon in the **Alert Name** column opens the **Alert Viewer** pop-up window, where detailed information about the triggered alert can be reviewed. The following elements are particularly relevant for investigation:



- *ENABLE ROW SELECTION* - Enables selection of multiple alerts for bulk actions.
  - *BULK MARK AS ACKNOWLEDGED* - Marks selected alerts as reviewed or acknowledged.
  - *BULK MARK AS FALSE POSITIVE* - Tags selected alerts as non-threats or incorrect detections.
  - *BULK MARK AS NEW* - Resets the status of selected alerts to “new”.
  - *RUN PLAYBOOK WITH ALERTS* - Executes an automated playbook using the selected alerts as input.
  - *BULK SET ALERT ASSIGNEE (USER)* - Assigns selected alerts to a specific user.
  - *BULK SET MITREID* - Assigns or updates the MITRE ATT&CK classification for selected alerts.
  - *ADD TO EXISTING INVESTIGATION* - Links the selected alert to a previously created investigation case.
  - *BULK SET USER CLASSIFICATION* - Updates the user classification for selected alerts.
  - *BULK DELETE* - Removes the selected alerts.
- *RUN PLAYBOOK* - Executes a predefined automated response procedure.
- *CREATE INVESTIGATION CASE* - Opens a new investigation case based on the alert.
- *VIEW ANOMALY EVENTS* - Opens the anomaly events associated with the selected alert.

  The following actions are available from the alert actions menu. To access them, open the alert details and click the

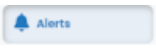
  on the right side of the alert action bar. The menu displays additional options for managing, classifying, exporting, or deleting the selected alert.

- *VIEW FULL ALERT* - Opens the complete alert details in a dedicated view.
- *ADD TO EXISTING INVESTIGATION* - Links the alert to a previously created investigation case.
- *DOWNLOAD* - Saves the alert details locally as a JSON file format.
- *EXPLAIN* - Opens the **CyberQuest Assistant** AI chat to provide contextual analysis and investigation guidance for the selected alert.
- *CHANGE USER CLASSIFICATION* - Updates the threat classification of the involved user.
- *MARK AS ACKNOWLEDGED* - Flags the alert as reviewed or noted.
- *MARK AS FALSE POSITIVE* - Tags the alert as a non-threat or incorrect detection.
- *MARK AS NEW* - Resets the alert status to “new” for further review.

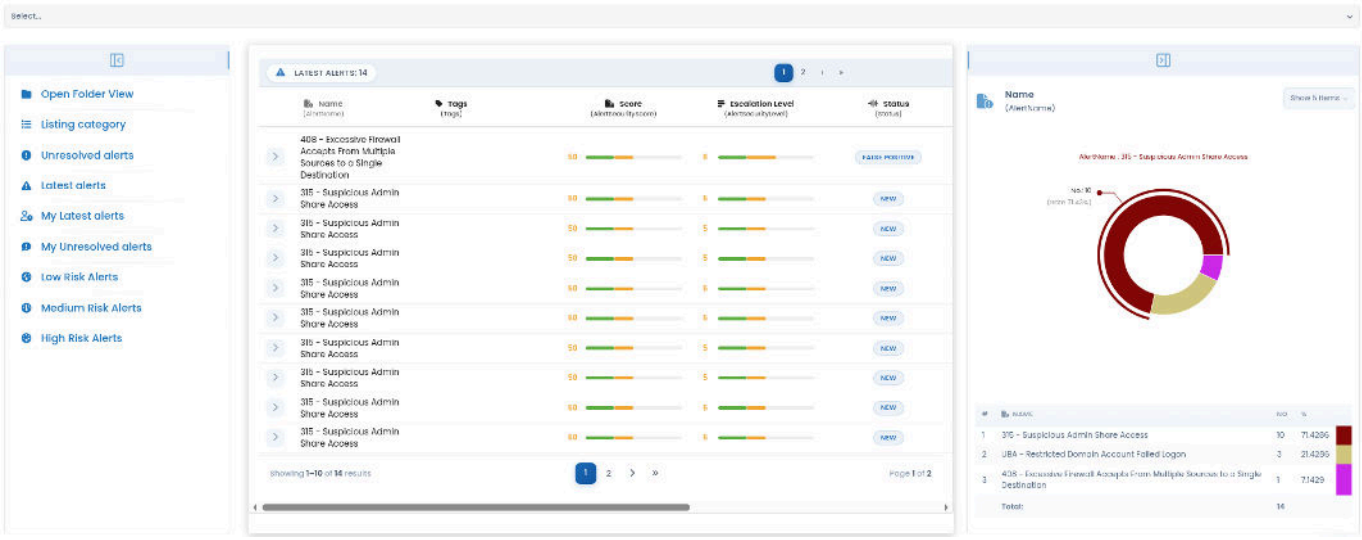
- *ADD DEDUPLICATE ITEM* - Marks this alert as a duplicate of another.
- *SET DEDUPLICATE OF* - Assigns another alert as the original this one duplicates.
- *DELETE* - Removes the alert.

Manage Alerts

To manage a triggered alert, open the **Alerts** module by clicking the



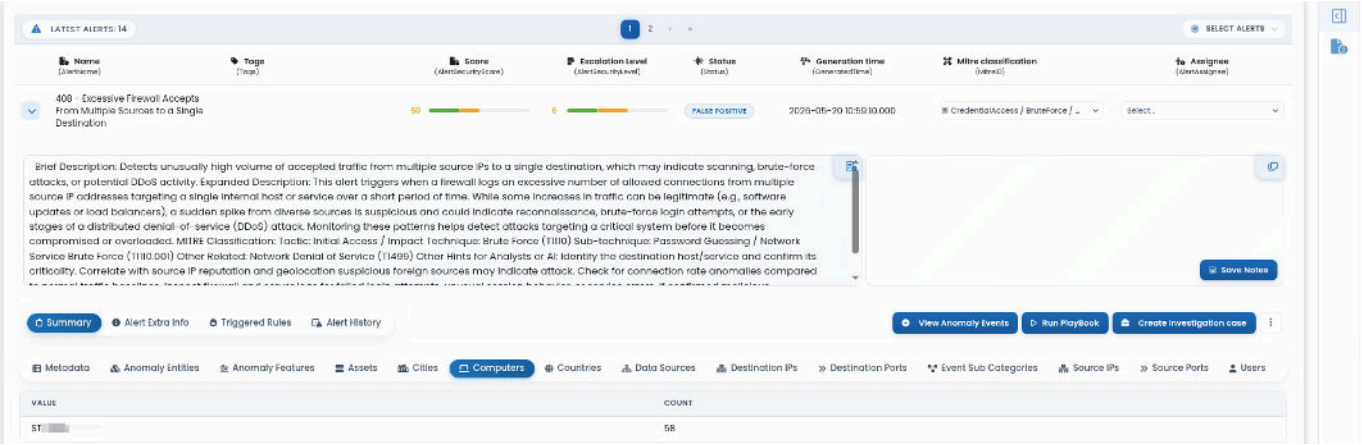
button located on the left-hand side of the web interface. This opens the alert management view, where triggered alerts can be reviewed, assigned, updated, exported, or removed.



Click the



icon in the **Alert Name** column to expand the selected alert. Once expanded, additional alert details are displayed directly in the **Alerts** view, including the alert description, notes area, response actions, summary information, related entities and investigation options.

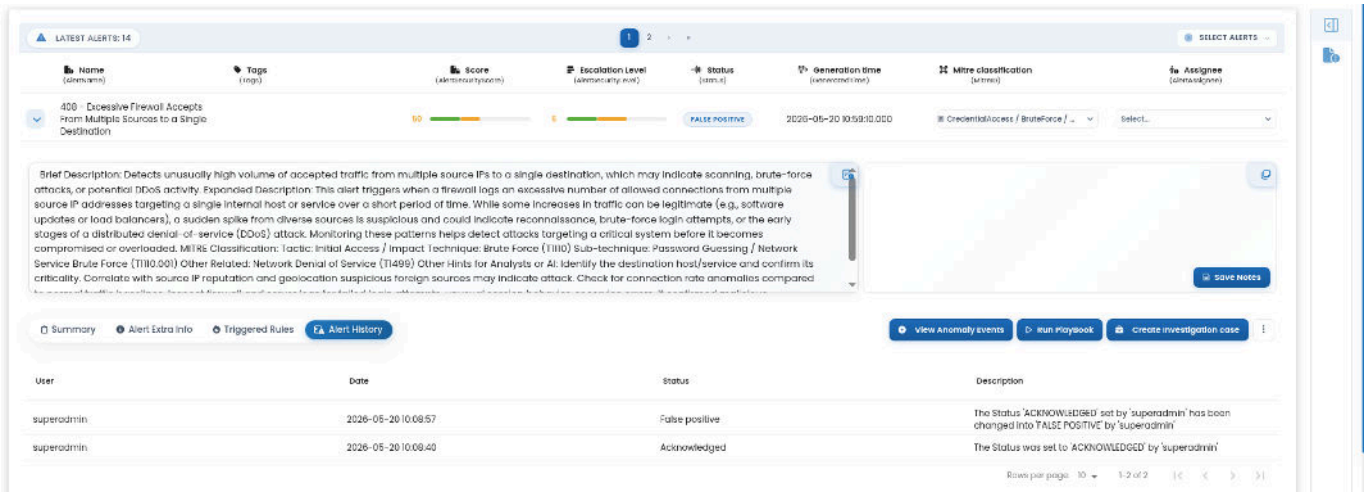


- The **Alert History** tab provides a chronological record of the actions performed on the selected alert. It displays information such as the user who performed the action, the date and time of the action, the updated alert status, and any related notes or comments.

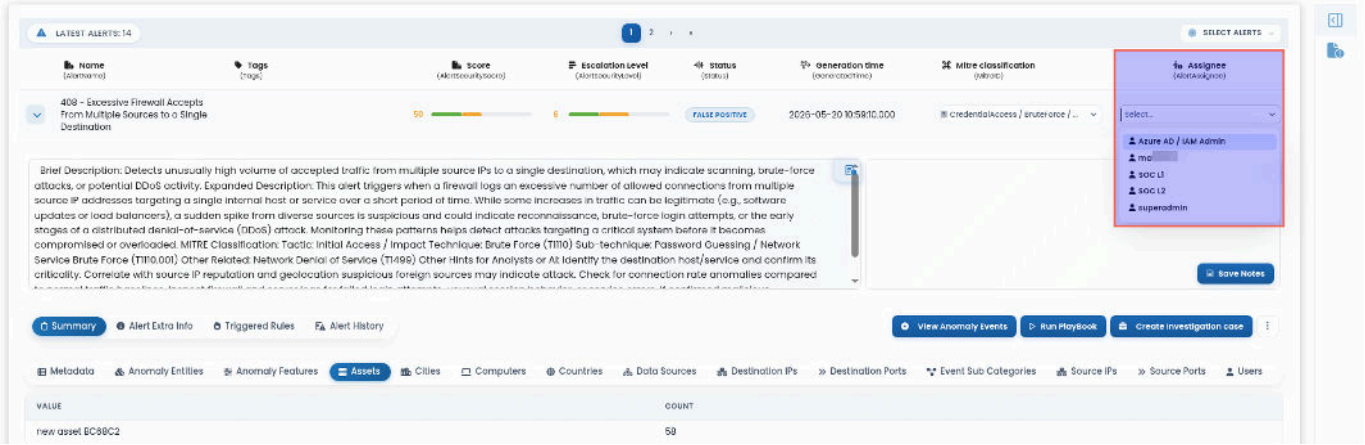
  Use the **Alert History** tab to review all management activities performed on the alert by clicking th

button:



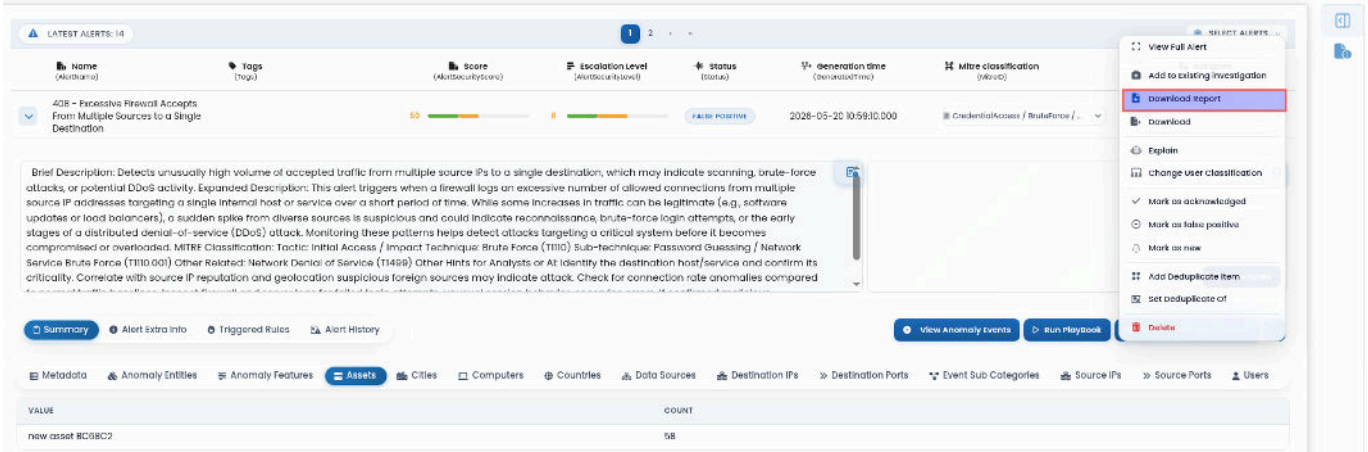
- Alerts can be assigned to specific users for investigation, follow-up, or resolution. This helps distribute alert handling responsibilities across analysts or team members:



- The **Download Report** action is available from the alert actions menu. To access it, open the alert details and click the

on the right side of the alert action bar. This option allows the user to export a report for the selected alert in HTML format.

DOWNLOAD REPORT - Downloads a generated report containing the details and context of the selected alert.



CYBERQUEST Alert History of 408 - Excessive Firewall Accepts From Multiple Sources to a Single Destination

AlertSecurityScore: 50
AlertSecurityLevel: 6

Alert History

Status	Field	User	Description	Date
ACKNOWLEDGED	Status	superadmin	The Status was set to 'ACKNOWLEDGED' by 'superadmin'	2026-05-20 10:08:40
FALSE POSITIVE	Status	superadmin	The Status 'ACKNOWLEDGED' set by 'superadmin' has been changed into 'FALSE POSITIVE' by 'superadmin'	2026-05-20 10:08:57

Note: In the exported HTML report, the **Date** field from the **Alert History** table is displayed in UTC time.

The **Run Playbook** action allows the user to manually select and execute a predefined response action from the available playbook list.

- **RUN PLAYBOOK** - Allows manual selection of an action from the playbook list to execute on the alert/event.

Alerts Manual Deduplication

Manual deduplication allows users to link duplicate or closely related alerts to a primary alert. This helps reduce repeated entries in the alert list, keeps related alerts grouped together, and supports faster investigation and correlation during analysis.

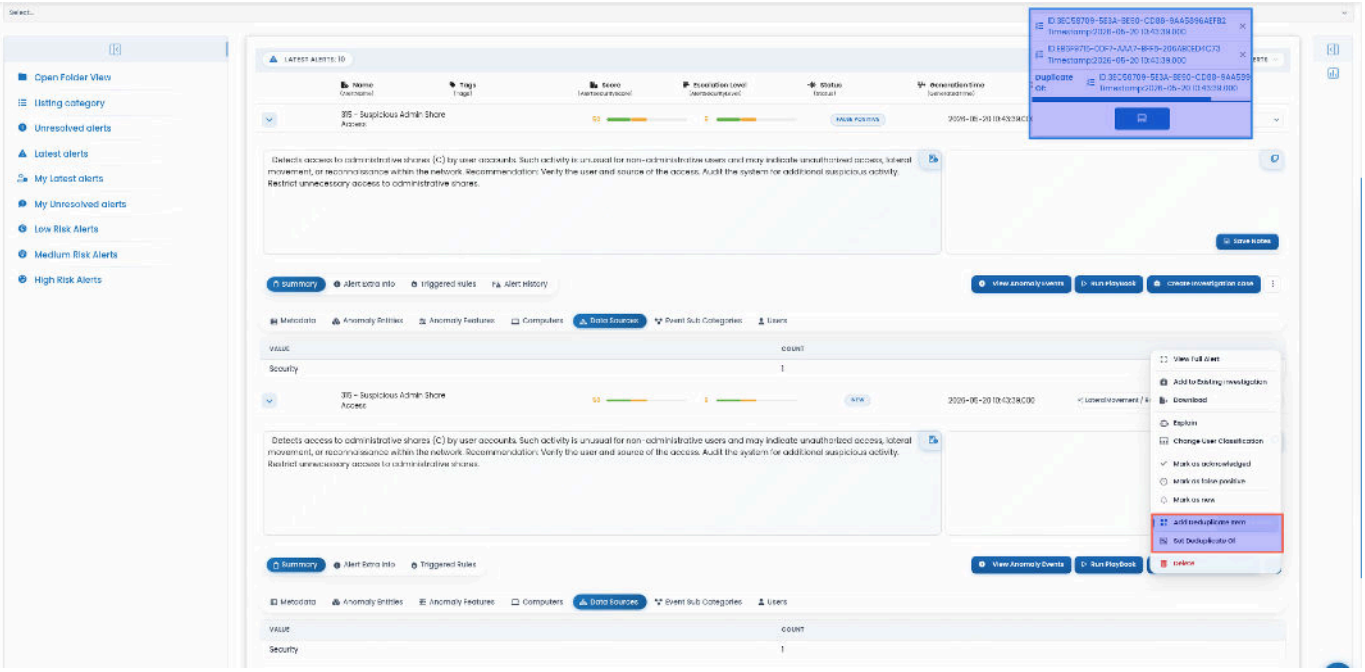
To manually deduplicate an alert:

1. Open the **Alerts** module.
2. Identify the alert that should be marked as a duplicate or linked to another alert.
3. Expand the alert details, then click the

   on the right side of the alert action bar.
4. First select **Add Deduplicate Item** to add the alert to the deduplication process.
5. After the duplicate item is added, select **Set Deduplicate Of** to define the primary/root alert to which the current alert will be linked.
6. In the deduplication selection window, review the selected alert and the **Duplicate Of** relation, then click the confirmation button

   to apply the deduplication link.



Deduplication Options:

- **Add Deduplicate Item**: Adds the selected alert as a deduplication item, preparing it to be linked to another related alert.
- **Set Deduplicate Of**: Defines the primary/root alert that the selected alert duplicates.

Once both actions are applied, the alert is associated with the selected primary alert. This helps analysts manage repeated detections more efficiently and avoid investigating the same activity multiple times.

Create Investigation Case

For detailed instructions on creating an investigation case, refer to the Case Management section.

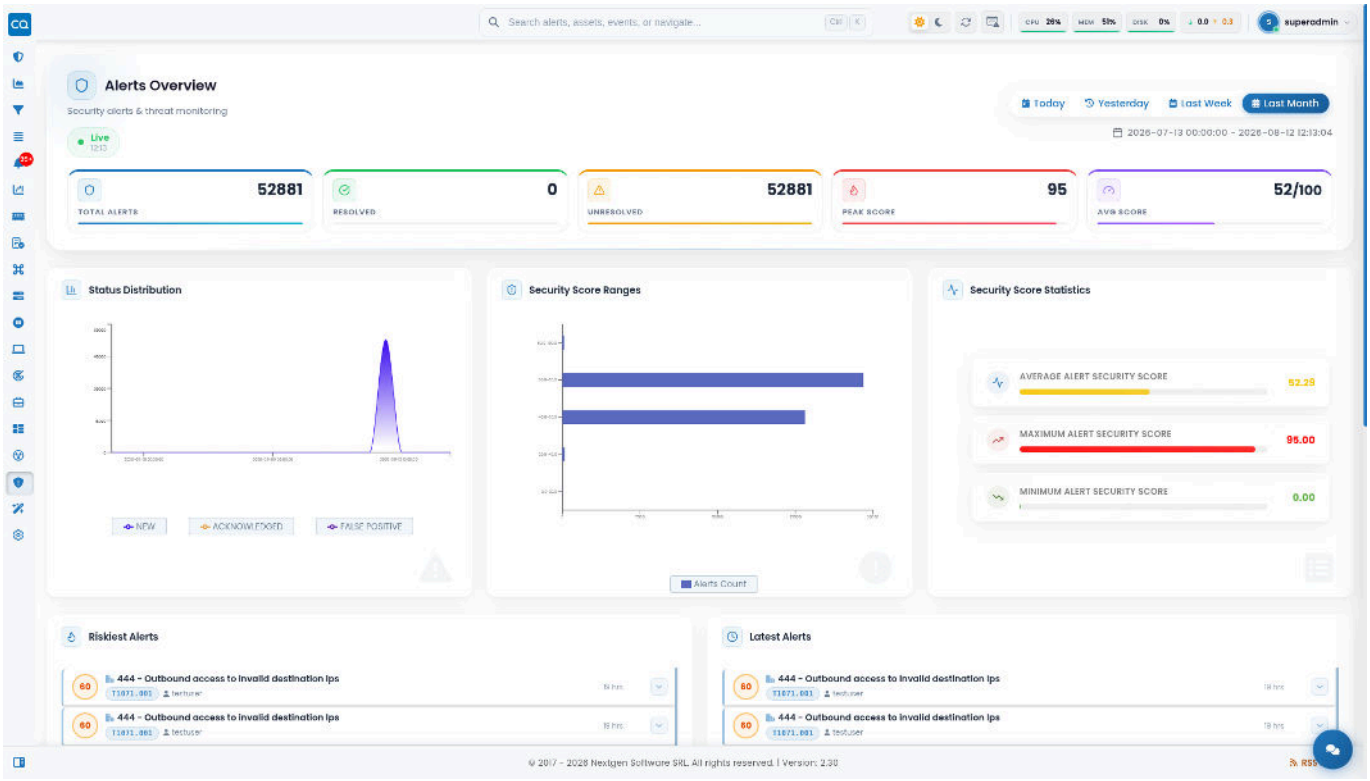
Alerts Overview

What the Alerts Overview shows

The **Alerts Overview** provides a consolidated view of alert activity, severity, status, and affected entities for the selected period.

It complements the **Alerts** module by presenting aggregated information and key indicators before you move into individual alert records.

To open the page, select **Alerts Overview** from the left-side navigation menu.



Select the analysis period

Use the period controls in the upper-right corner to define the time window analyzed by the page:

- **Today**
- **Yesterday**
- **Last Week**
- **Last Month**

The selected period is highlighted, and the exact start and end timestamps are displayed below the selector.

All period-based KPIs, charts, and alert lists are updated according to the selected interval.

The **Live** indicator shows that the page is active and displays the current time.

Alert summary

The KPI cards at the top of the page provide a quick summary of alert activity for the selected period:

- **Total Alerts** - total number of alerts recorded during the selected period.
- **Resolved** - number of alerts with a resolved status.
- **Unresolved** - number of alerts that remain unresolved.
- **Peak Score** - highest alert security score recorded during the period.
- **Avg Score** - average alert security score calculated across the alerts in the selected period.

The security score indicators provide a quick view of the overall severity represented by the alert population.

Alert status and security score analysis

The next section provides a visual breakdown of alert status and security scores.

Status Distribution

Status Distribution shows how alert activity is distributed across alert statuses during the selected period.

The available statuses can include:

- **NEW**

- **ACKNOWLEDGED**
- **FALSE POSITIVE**

Use this view to understand how alert activity and processing status evolve over time.

Security Score Ranges

Security Score Ranges groups alerts according to their security score.

The chart makes it possible to compare the volume of alerts across different score intervals and quickly determine where most alerts are concentrated.

Higher score ranges represent alerts with a higher calculated security score.

Security Score Statistics

Security Score Statistics provides three numerical indicators for the selected period:

- **Average Alert Security Score**
- **Maximum Alert Security Score**
- **Minimum Alert Security Score**

These values complement the score-range distribution by showing the overall minimum, maximum, and average score across the analyzed alerts.

Riskiest and Latest Alerts

The **Riskiest Alerts** and **Latest Alerts** panels provide two different perspectives on individual alerts.

Riskiest Alerts highlights alerts with the highest security scores, helping identify alerts with the greatest calculated severity.

Latest Alerts shows the most recently generated alerts, providing visibility into the latest activity detected by the platform.

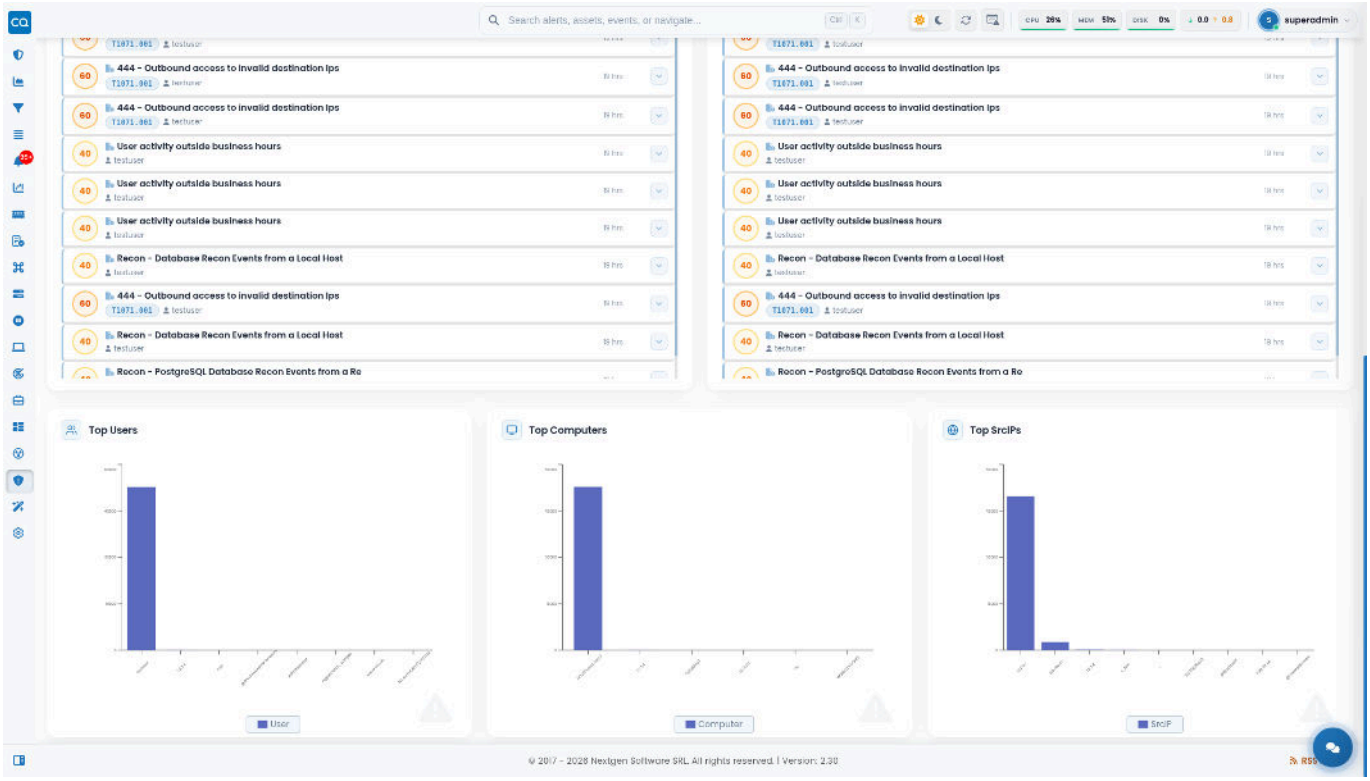
Alert entries can include information such as:

- alert security score;
- alert name;
- MITRE ATT&CK technique, when available;
- associated user or entity;
- alert timestamp.

This allows you to move from the aggregated dashboard view to individual alerts that require further analysis.

Top affected entities

The lower section of the page identifies the entities that appear most frequently in alerts during the selected period.



The lower section of the page identifies the entities that appear most frequently in alerts during the selected period.

Three charts are available:

- **Top Users** - users most frequently associated with alerts.
- **Top Computers** - computers most frequently associated with alerts.
- **Top SrcIPs** - source IP addresses most frequently associated with alerts.

These views help identify entities that are repeatedly involved in alert activity and can provide useful starting points for further investigation.

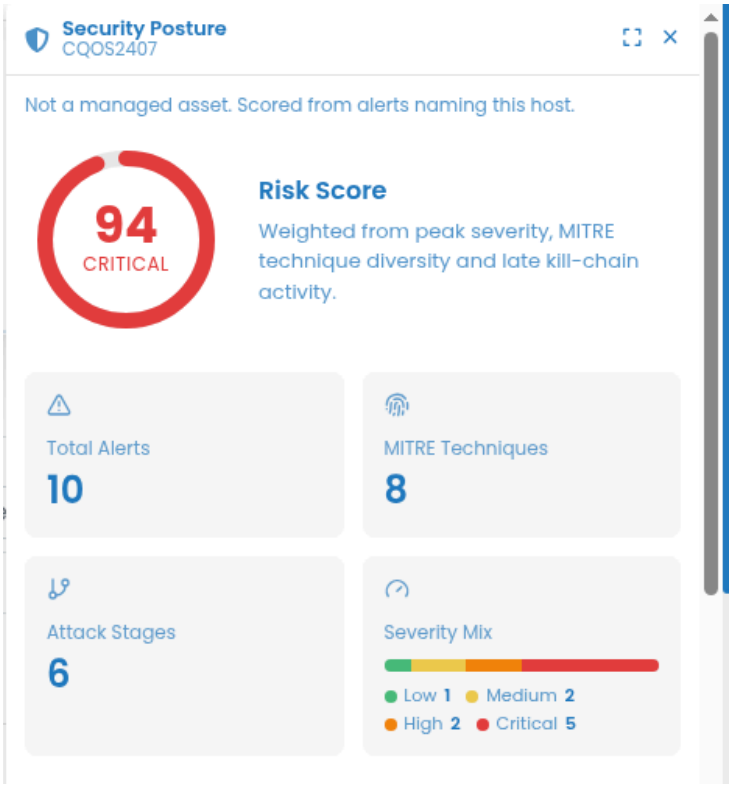
Security Posture

What the security posture shows

The security posture answers a single question about one machine: **how bad does this host look right now?**

CYBERQUEST reads every alert raised against a host over the selected period and summarises it as a risk score from 0 to 100, where a higher score is worse. Alongside the score you get the kill-chain stages the host has been through, the MITRE ATT&CK techniques seen against it, how its alerts break down by severity, and the alerts themselves.

The posture is not a separate module you navigate to. It opens **wherever a computer name or an IP address appears** — on an alert, on an event, or on a device discovered by the Data Scanner — so you can check a host without losing your place.



Reading the panel

The panel is laid out top to bottom, from verdict to evidence.

Risk Score is the headline. The dial shows the 0–100 value and its band: **Minimal**, **Low**, **Moderate**, **Elevated** or **Critical**. The score is weighted from three things — the peak severity of the host's alerts, how many distinct MITRE techniques were seen against it, and how far along the kill chain those techniques sit. A host with one very severe alert scores lower than a host showing several different behaviours across late kill-chain stages.

Under the dial, four tiles give the counts behind the score:

- **Total Alerts** — how many alerts named this host in the period.
- **MITRE Techniques** — how many distinct techniques were seen.
- **Attack Stages** — how many kill-chain stages the host has touched.
- **Severity Mix** — the split across Low, Medium, High and Critical, as a bar with the count for each band.

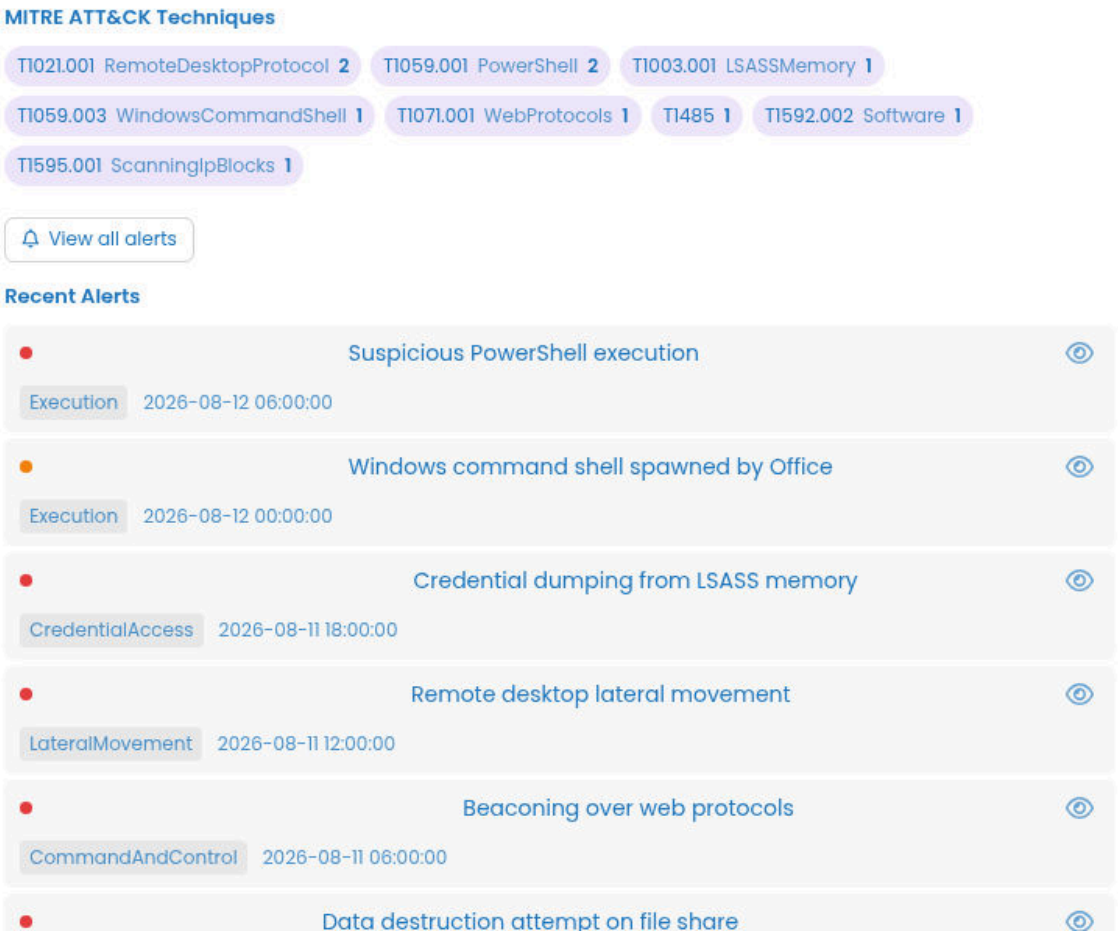
Attack Stages lists the kill-chain stages with the number of alerts in each — for example **Execution**, **CredentialAccess**, **LateralMovement**, **CommandAndControl**, **Impact**. Stages are derived from the MITRE technique on each alert, so an alert with no technique contributes no stage.

MITRE ATT&CK Techniques lists the individual techniques with their identifier and name, such as `T1003.001 LSASSMemory` or `T1059.001 PowerShell`.

Recent Alerts shows the most recent alerts for the host, each with its kill-chain stage and the time it was generated. Use it to jump from the summary to what actually happened.

Opening the alerts behind the score

The panel summarises the alerts; when you need the alerts themselves, two controls take you to them.



Each row in **Recent Alerts** carries an eye. Click it to open **that single alert** in the Alerts module, with everything recorded about it — its tabs, MITRE technique, affected computers and users, and the rules it triggered.

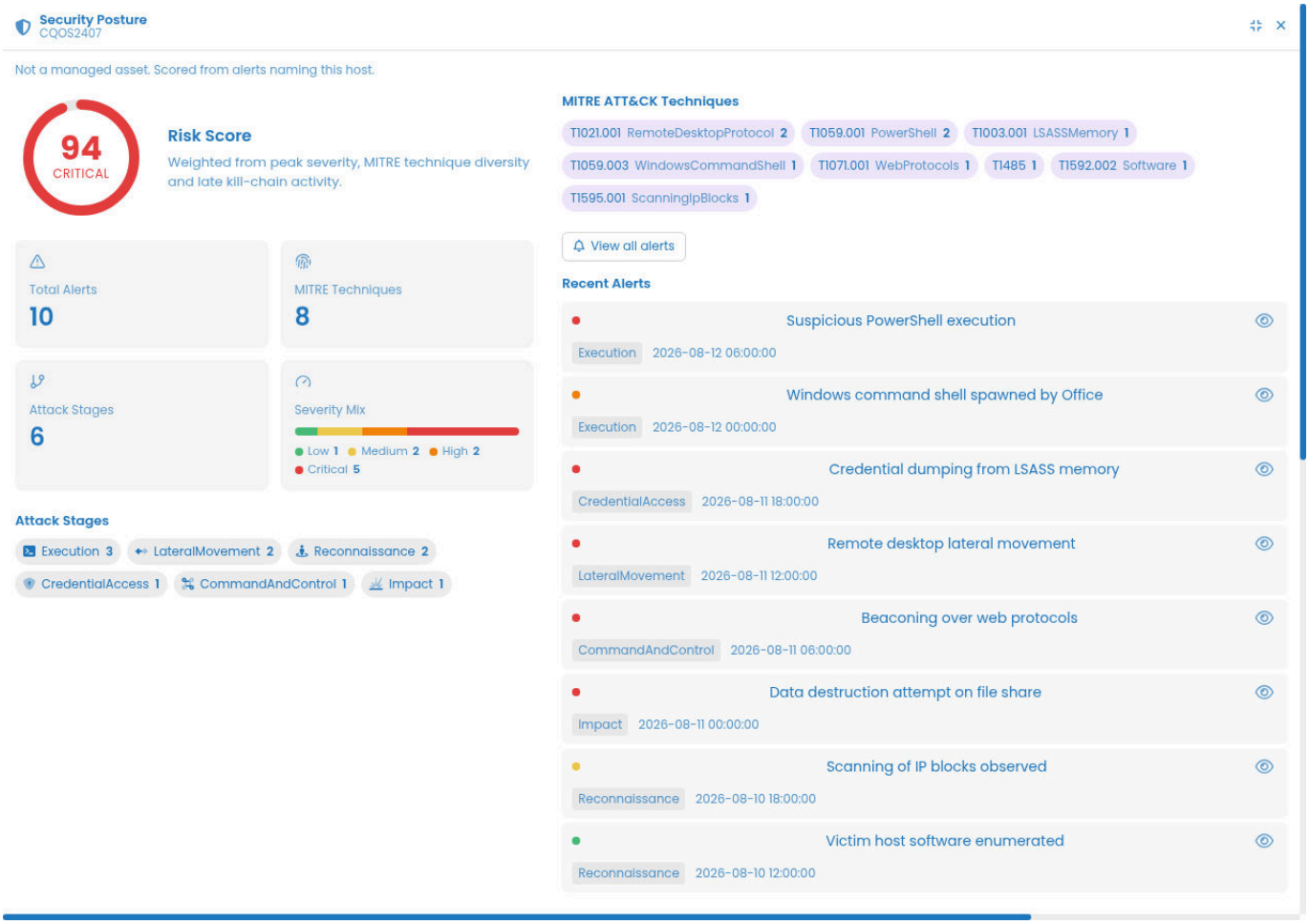
The **View all alerts** button opens **every alert for this host** in the Alerts module instead.

Both open in a **new browser tab**, so the page you came from stays where it was — the device list, the event you were reading, or the alert you were triaging. Both also carry the same seven-day period the score was calculated over, so the number of alerts in the list matches the **Total Alerts** count in the panel.

Directly under the host name, the panel tells you whether the machine is in your asset inventory — either **Managed asset** followed by the asset name, or **Not a managed asset**, meaning the score was calculated purely from alerts naming that host.

Working in a wider view

The panel opens docked at the right of the screen so the page behind it stays usable. Press the expand button in the panel header to take it full screen, which puts the verdict and counts on the left and the technique list and recent alerts on the right.

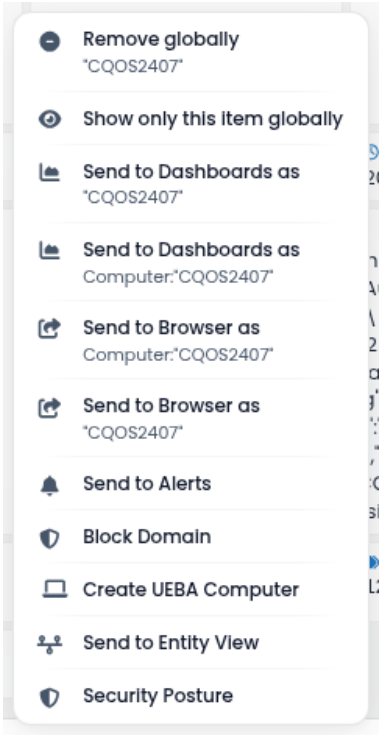


Press the same button again to return it to the docked size. Press **Esc** or the close button to dismiss it.

Opening the security posture

From an event in the Browser

In the Browser, open an event and click the value of the **Computer** or **SrcIP** field. The actions menu opens; choose **Security Posture** at the bottom.



The same menu appears wherever those fields are shown, so the posture is always one click from a host name.

From an alert

Open an alert and select the **Computers** tab — or **SrcIPs** for an address. Click any value in the list to open its posture.

This is the quickest route when you are triaging: the alert tells you what happened once, the posture tells you what else has happened to the same machine.

From a discovered device

Under **Settings › Application › Data Scanner**, open the **Devices** tab. Each row ends with a set of actions; the shield is the security posture.



The other two icons in that group open the device's performance metrics and its CMDB details — the shield is the rightmost of the three.

Key Considerations

The period is the last seven days. The panel always scores the host over the previous week. A host that was noisy a month ago and quiet since will show a low score.

No alerts is a valid answer. If the host has no alerts in the period, the panel says *No security alerts in this window* rather than showing a score of zero. That is a clean bill of health for the week, not an error.

Hostnames and addresses are matched exactly. If the host is in your asset inventory, CYBERQUEST also matches the other names recorded for that asset — its display name, hostname, FQDN and IP address — so alerts filed under any of them are counted.

Masked values cannot be scored. If your account does not have the **Decrypt Sensitive Event Data** permission, computer names in events are shown as protected values beginning `cqenc:`. Those cannot be resolved to a host, so no **Security Posture** action is offered for them. Ask an administrator to grant the permission if you need to work with real host names.

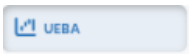
Access. The posture is built entirely from alert data, so it requires the **View Alerts** permission.

Ueba Module

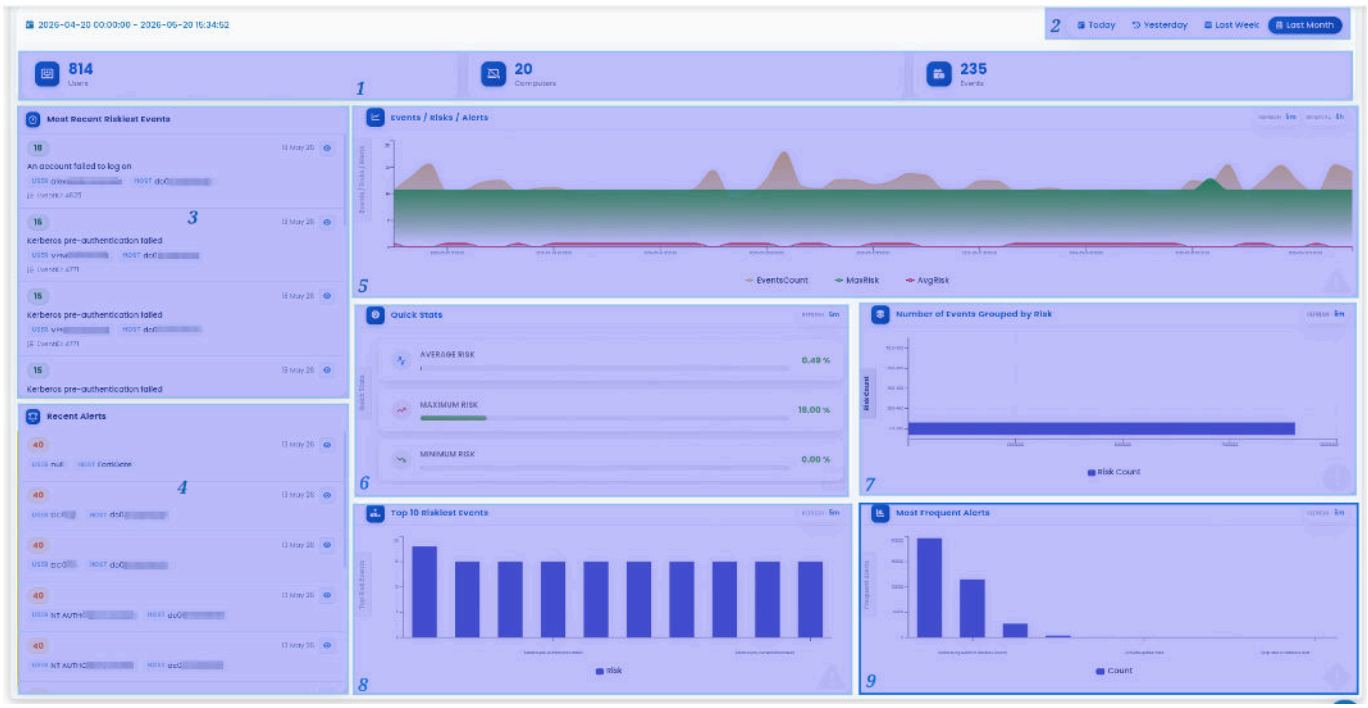
The **UEBA (User and Entity Behavior Analytics) module** helps security teams identify suspicious or unusual behavior across monitored users and computers. It consolidates events, alerts, risk scores, and behavioral indicators into a centralized view, allowing analysts to quickly prioritize risky activity and investigate the entities involved.

When anomalous behavior is detected, UEBA can generate alerts and assign risk scores to the relevant events. These indicators help analysts understand which users or computers require attention and support faster investigation and response.

Access the **UEBA module** by clicking the



button in the left-side panel of the Web Interface.



UEBA Dashboard

The UEBA dashboard provides an operational overview of risky behavior detected in the monitored environment. It highlights affected users, computers, alerts, and events, and provides quick access to detailed event and entity-level investigation views.

1 - **Risk Counters**
Displays the number of users, computers, and events with a risk score higher than zero.

2 - **Time Interval Selection**
Allows selection of the time interval for viewing high-risk events: **Today, Yesterday, Last Week, or Last Month**.

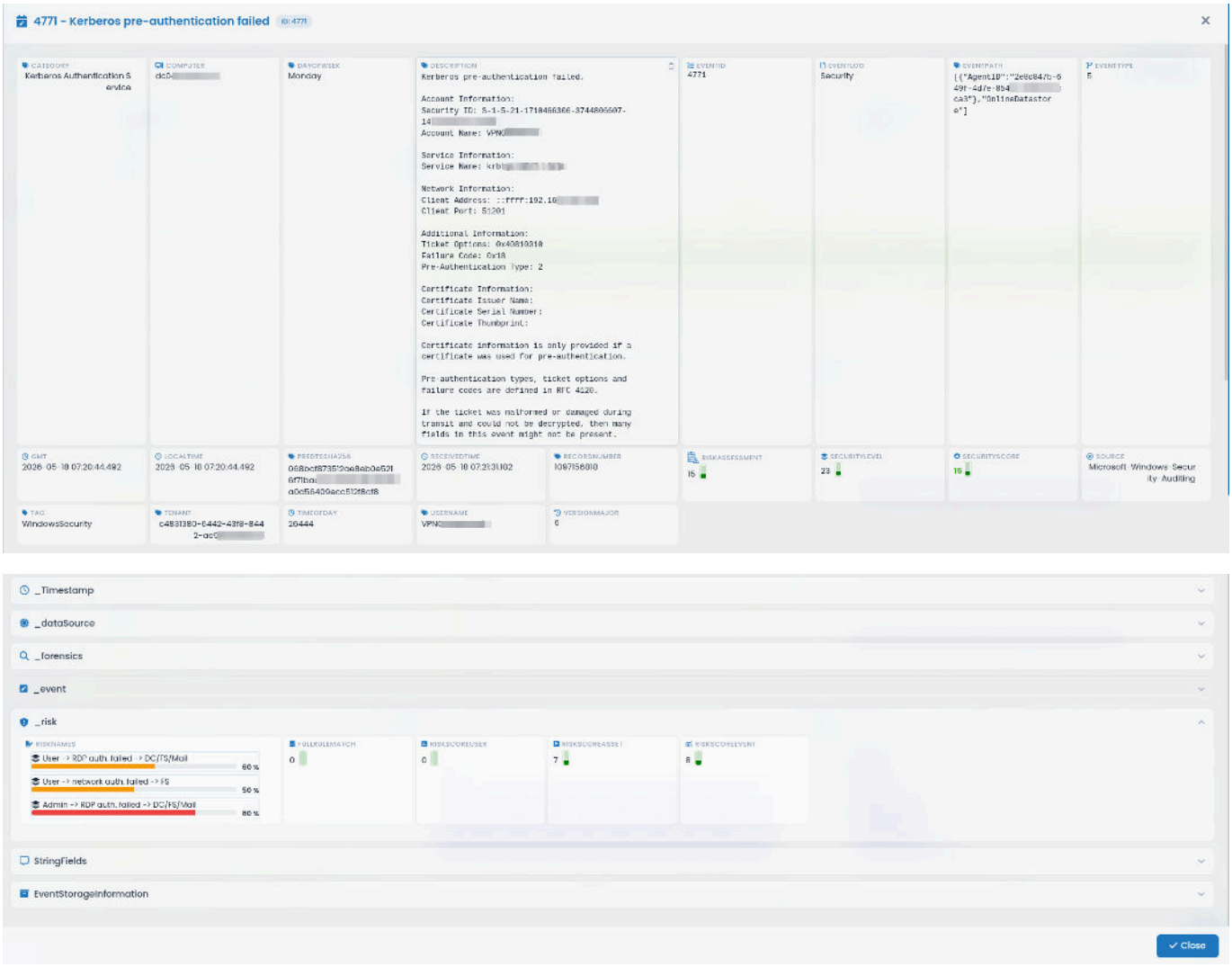
3 - **Top 10 Riskiest Events**

Lists the events with the highest risk scores for the selected time interval. Risk levels are color-coded for quick prioritization:

- **Green** indicates low risk.
- **Yellow** indicates medium risk.
- **Red** indicates high risk.

To view the full details of an event, click the

button. The event details page opens with the associated event information.

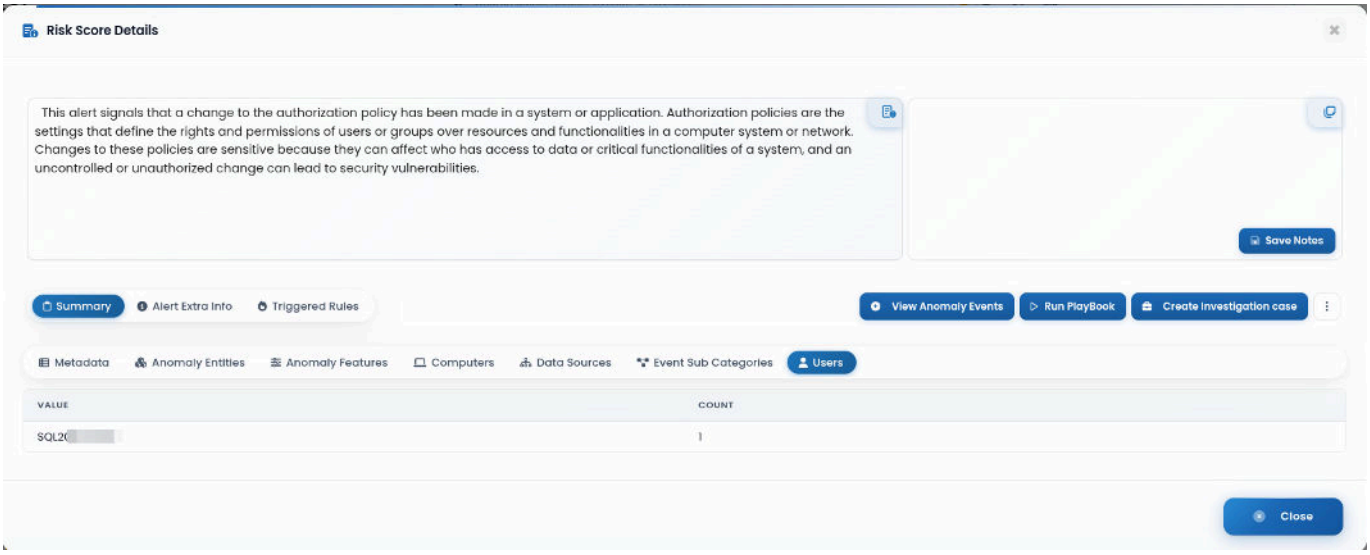


4 - **Top 10 Riskiest Alerts**

Lists the Top 10 riskiest alerts.

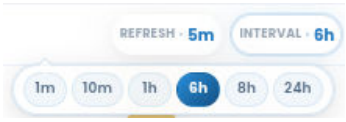
Lists the alerts with the highest associated risk scores. To view the risk score details for a recent alert, click the

button.



5 - **Events / Risks / Alerts Chart**

Displays the number of events together with the maximum and average risk levels identified during the selected interval. The chart is displayed using sample data points. The automatic refresh interval can be set to **1 minute**, **5 minutes**, or **OFF**.



6 - **Quick Stats**

Displays the maximum, minimum, and average risk percentages. The automatic refresh interval can be set to **1 minute**, **5 minutes**, or **OFF**.

7 - **Number of Events Grouped by Risk**

Shows how many events are associated with each risk level. The automatic refresh interval can be set to **1 minute**, **5 minutes**, or **OFF**.

8 - **Top 10 Riskiest Events Chart**

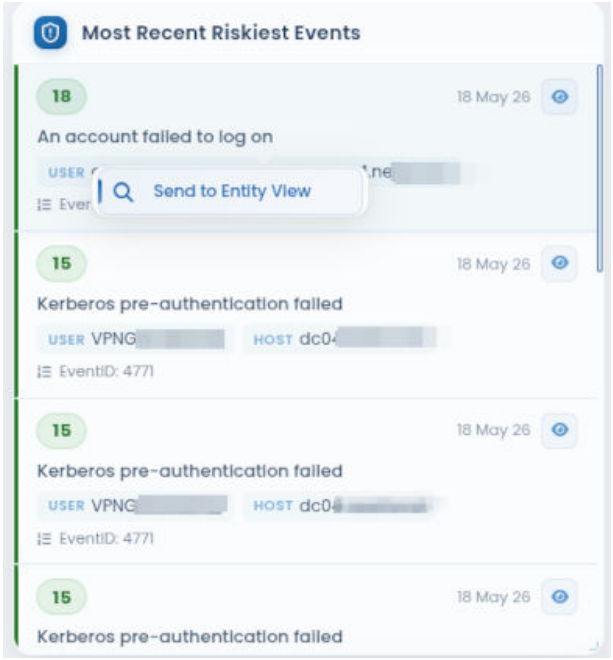
Displays a graphical view of the highest-risk events. The automatic refresh interval can be set to **1 minute**, **5 minutes**, or **OFF**.

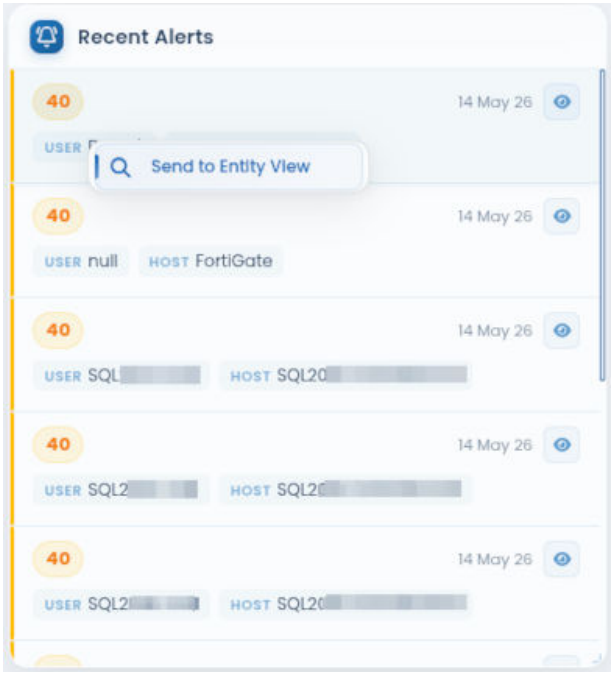
9 - **Most Frequent Alerts**

Displays the alerts that occurred most frequently in the selected time interval. The automatic refresh interval can be set to **1 minute**, **5 minutes**, or **OFF**.

Opening the Entity View

From the **Recent Alerts** and **Most Recent Riskiest Events** sections, analysts can open the activity view for the related user or computer.





Click ***Send to Entity View*** to open a dedicated investigation page for the selected user or computer. The Entity View displays the activity stream, risk context, alerts, and related events for that entity.

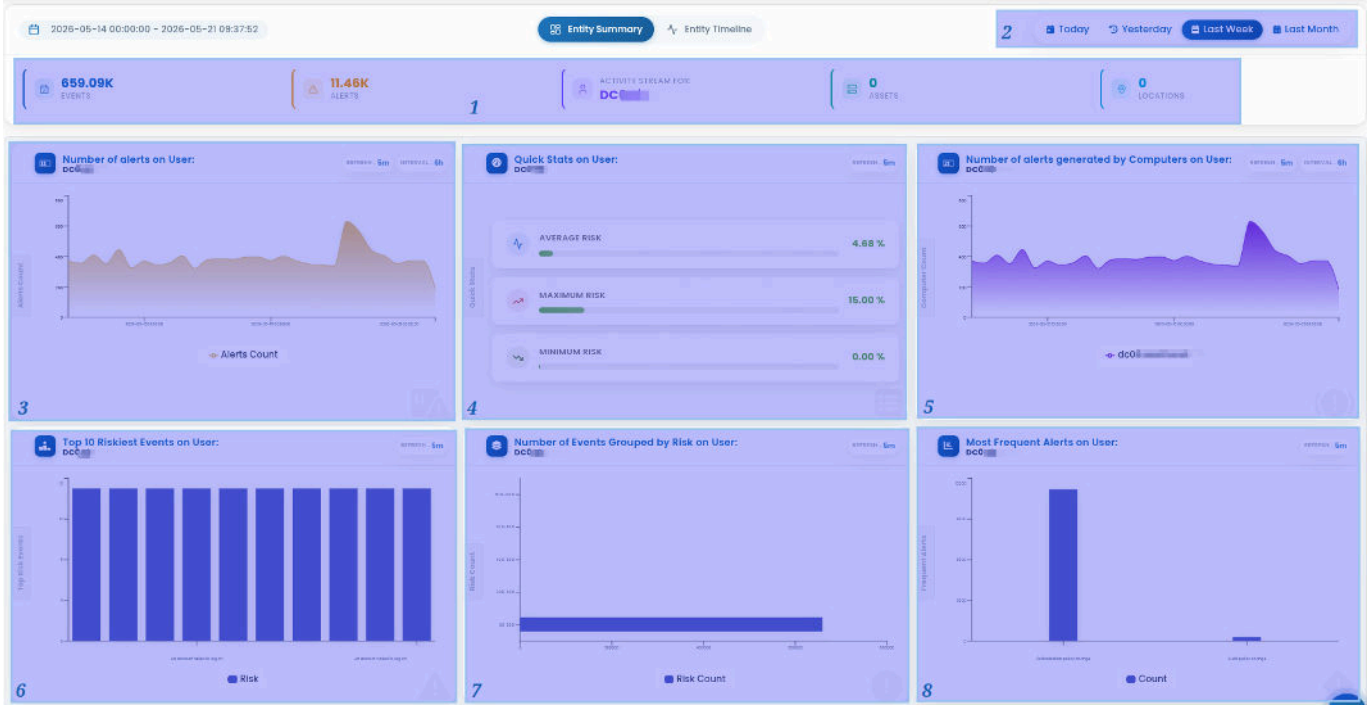
Entity View

The **Entity View** provides an investigation-focused view for a selected user or computer. It contains two main perspectives:

- **Entity Summary** - a dashboard-style overview of risk, alerts, events, and related entities.
- **Entity Timeline** - a chronological activity stream that helps analysts reconstruct behavior over time.

User Entity Summary

The **User Entity Summary** provides a high-level overview of a selected user's activity, risk posture, and behavioral patterns. It consolidates recent alerts, risk scores, notable events, and related entities into a single view, helping analysts identify deviations from expected behavior and decide where to investigate next.

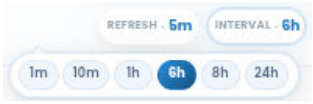


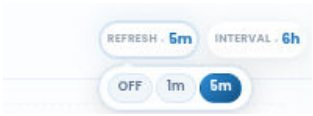
1 - **User-Linked Entities Overview** Displays the total number of events, alerts, assets, and locations associated with the selected user during the specified time frame.

2 - **Time Interval Selection**

Allows selection of the time interval used for user risk analysis: **Today**, **Yesterday**, or **Last Week**.

3 - **User Alert Volume** Displays the number of alerts linked to the selected user during the chosen time interval. Refresh controls allow automatic updates every **1 minute** or **5 minutes**, or can be set to **OFF**.





4 - **User Quick Stats** Displays the maximum, minimum, and average risk percentages calculated for the selected user. Refresh controls allow automatic updates every **1 minute** or **5 minutes**, or can be set to **OFF**.

5 - **Alert Generation Over Time** Shows how many alerts were generated for the selected user by related computers. The chart can be displayed across configurable time intervals: **1 minute**, **10 minutes**, **1 hour**, **6 hours**, **8 hours**, or **24 hours**. Refresh controls allow automatic updates every **1 minute** or **5 minutes**, or can be set to **OFF**.

6 - **Top 10 Riskiest Events on User** Lists the most critical events associated with the selected user, based on risk score. Refresh controls allow automatic updates every **1 minute** or **5 minutes**, or can be set to **OFF**.

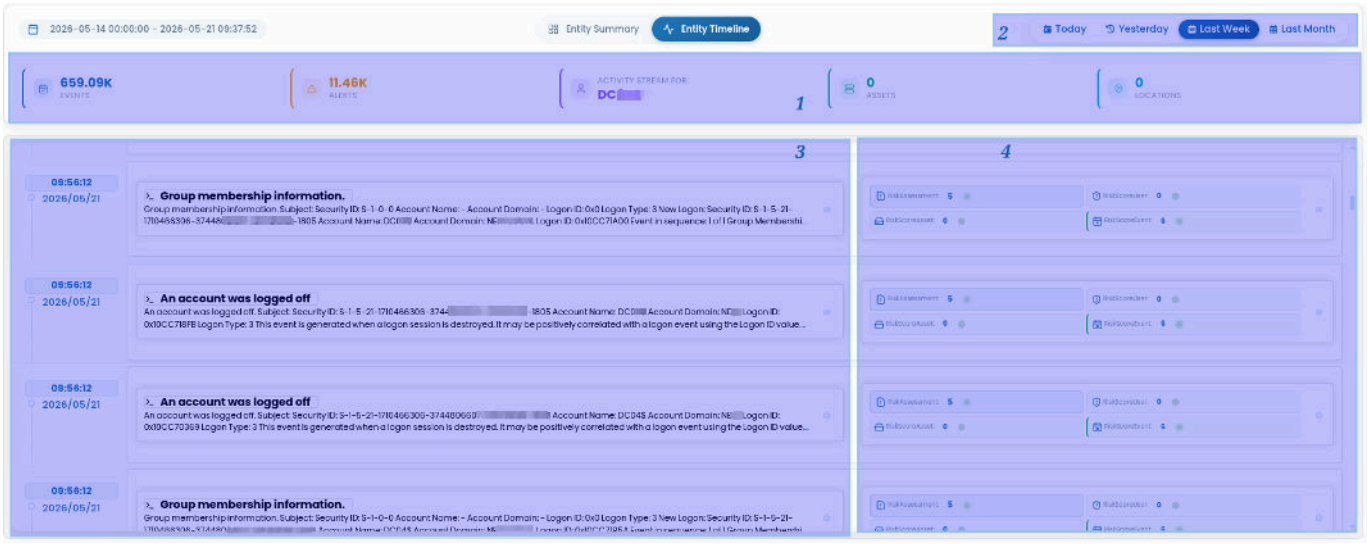
7 - **Event Count by Risk Level** Displays the number of user-related events grouped by risk category. Refresh controls allow automatic updates every **1 minute** or **5 minutes**, or can be set to **OFF**.

8 - **Most Frequent User Alerts** Highlights the alerts most frequently triggered for the selected user. Refresh controls allow automatic updates every **1 minute** or **5 minutes**, or can be set to **OFF**.

User Entity Timeline

The **User Entity Timeline** provides a chronological view of notable activities performed by, or associated with, the selected user. The timeline aggregates events such as logons, access attempts, triggered alerts, risk changes, and interactions with systems or assets.

This view helps analysts trace user behavior over time, identify suspicious patterns, and correlate events with risk scores and alerts during an investigation.



1 - **User Activity Counters**

Displays the total number of events, alerts, assets, and locations associated with the user during the selected time frame.

2 - Allows selection of the time interval used for risk-related activity analysis, such as **Today**, **Yesterday**, or **Last Week**.

3 - **Risk Event Timeline**

Shows all events identified as having a risk component, presented in chronological order. To examine the details of a specific event, click the

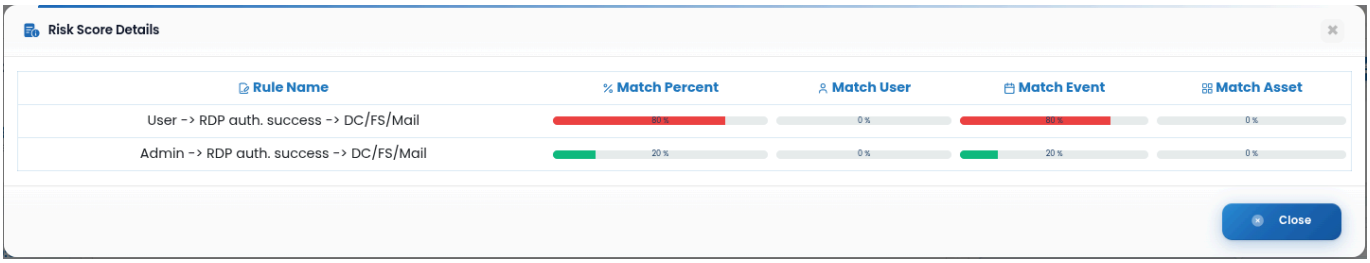
button.

4 - **Risk Score Details**

Shows how events are evaluated based on predefined detection patterns and logical evaluation methods. Matching events receive risk scores that help analysts prioritize the investigation.

To view the **risk score details**, click the

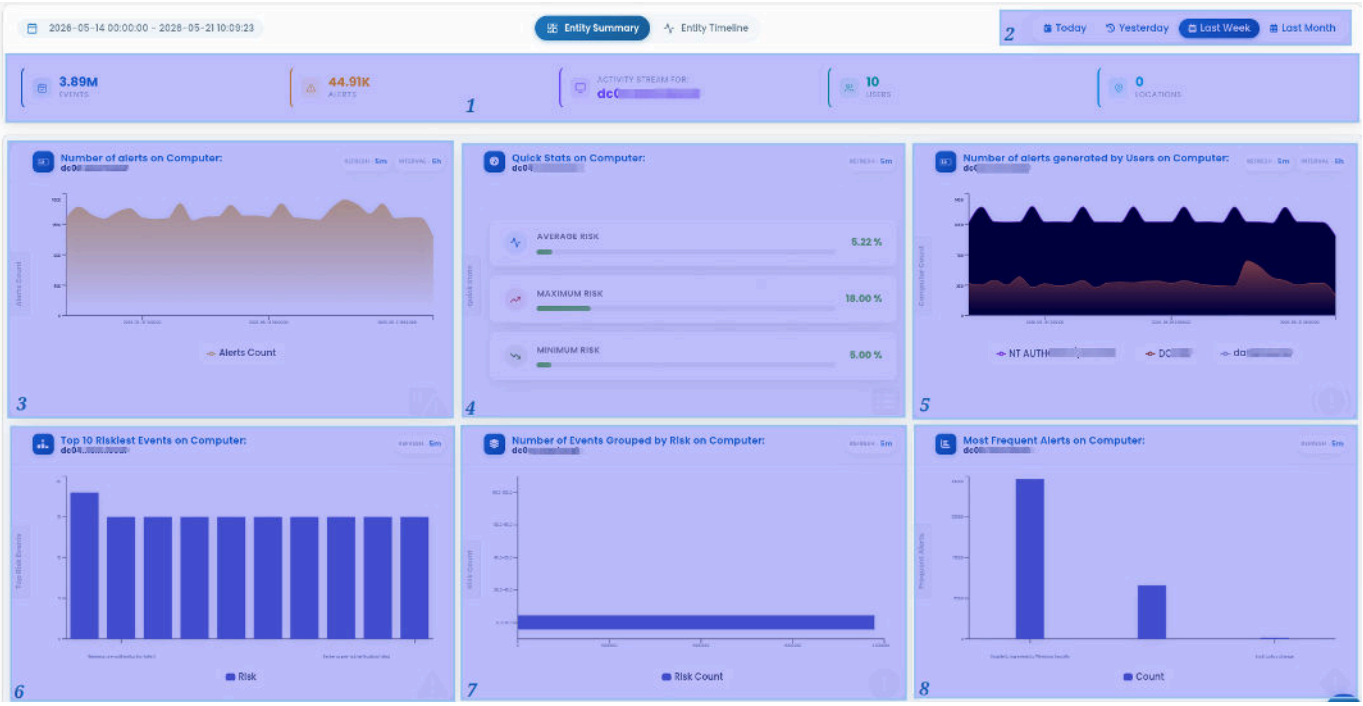
button to open the corresponding details page.



In the **Rule Name** field, the patterns defined in the **UEBA Manager** are displayed.

Computer Entity Summary

The **Computer Entity Summary** provides a consolidated overview of activity related to a selected computer. It displays key metrics and visualizations that help analysts assess the computer's involvement in security events, alert generation, risk levels, and interactions with users, assets, and network locations.



1 - **Event Summary**

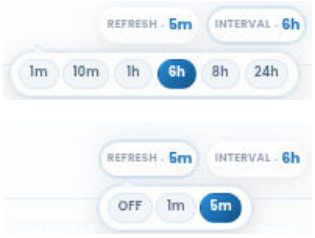
Displays the total number of events, alerts, users, and locations associated with the computer during the selected time frame.

2 - **Time Range Filter**

Allows selection of the analysis window used to display computer-related risk events: **Today**, **Yesterday**, or **Last Week**.

3 - **Alert Volume on Computer**

Displays the number of alerts linked to the selected computer within the chosen time interval. Refresh controls allow automatic updates every **1 minute** or **5 minutes**, or can be set to **OFF**.



4 - **Quick Stats on Computer**

PrDisplays the maximum, minimum, and average risk scores associated with the selected computer. Refresh controls allow automatic updates every **1 minute** or **5 minutes**, or can be set to **OFF**.

5 - **Alert Generation Over Time**

Shows how many alerts were triggered by the selected computer over configurable time intervals: **1 minute**, **10 minutes**, **1 hour**, **6 hours**, **8 hours**, or **24 hours**. Refresh controls allow automatic updates every **1 minute** or **5 minutes**, or can be set to **OFF**.

6 - **Top 10 Riskiest Events**

Highlights the ten highest-risk events involving the selected computer. Refresh controls allow automatic updates every **1 minute** or **5 minutes**, or can be set to **OFF**.

7 - **Risk-Based Event Distribution**

Displays the number of events grouped by risk level for the selected computer. Refresh controls allow automatic updates every **1 minute** or **5 minutes**, or can be set to **OFF**.

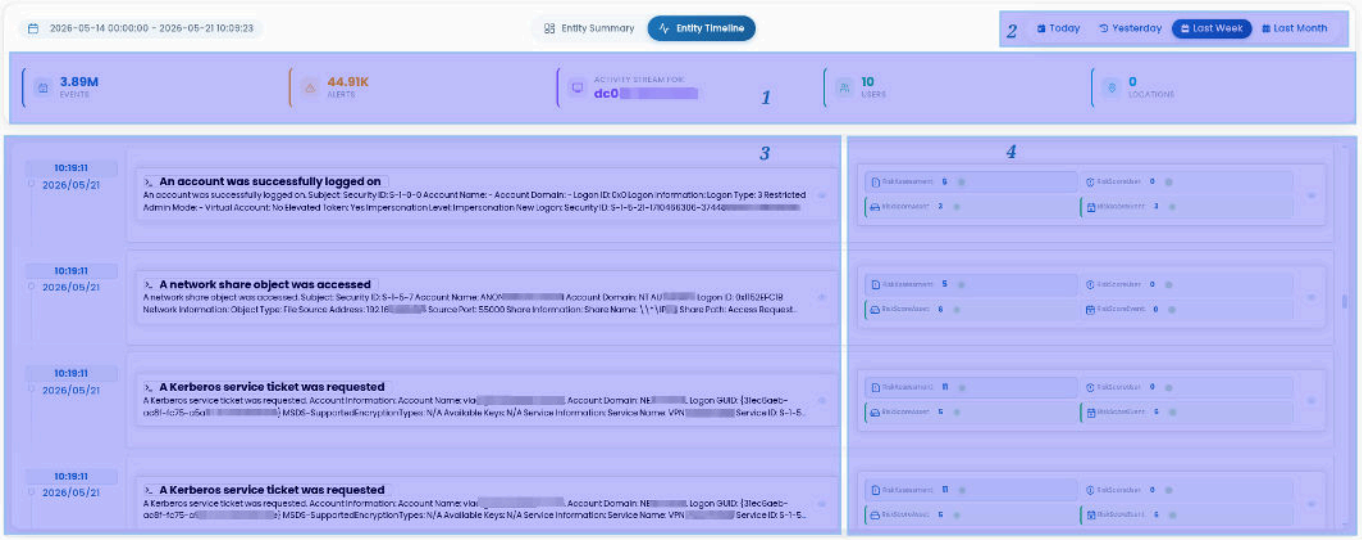
8 - **Most Frequent Alerts**

Lists the alerts most frequently associated with the selected computer. Refresh controls allow automatic updates every **1 minute** or **5 minutes**, or can be set to **OFF**.

Computer Entity Timeline

The **Computer Entity Timeline** provides a chronological activity stream for the selected computer. It helps analysts trace system behavior and correlate events over time, including alerts, user interactions, location changes, and other event-based activity involving the computer.

Each timeline entry is enriched with contextual metadata such as timestamps, event types, severity indicators, risk scores, and triggering rules. This enables faster identification of anomalous or risky activity.



1 - **Computer Activity Counters**

Displays the number of events, alerts, users, and locations associated with the selected computer during the specified time range.

2 - **Time Interval Selection**

Allows selection of the time interval used to analyze computer-related risk activity.

3 - **Risk Event Timeline**

Shows all events with an assigned risk factor, sorted in chronological order. To review a specific event, click the

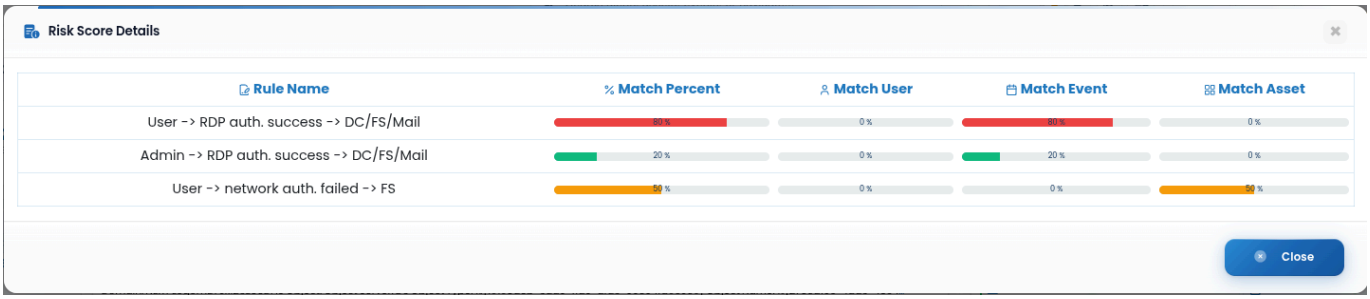
.

4 - **Risk Score Details**

Shows how events are evaluated using predefined detection rules or behavioral patterns. Each matching event is assigned a risk score based on severity and context.

To review the **risk score details**, click the

button. This opens the detailed risk analysis page.



Performance Module

The **Performance** module provides real-time and historical system performance insights for monitored machines. It is accessible by clicking the



button in the left-hand navigation panel of the Web Interface.

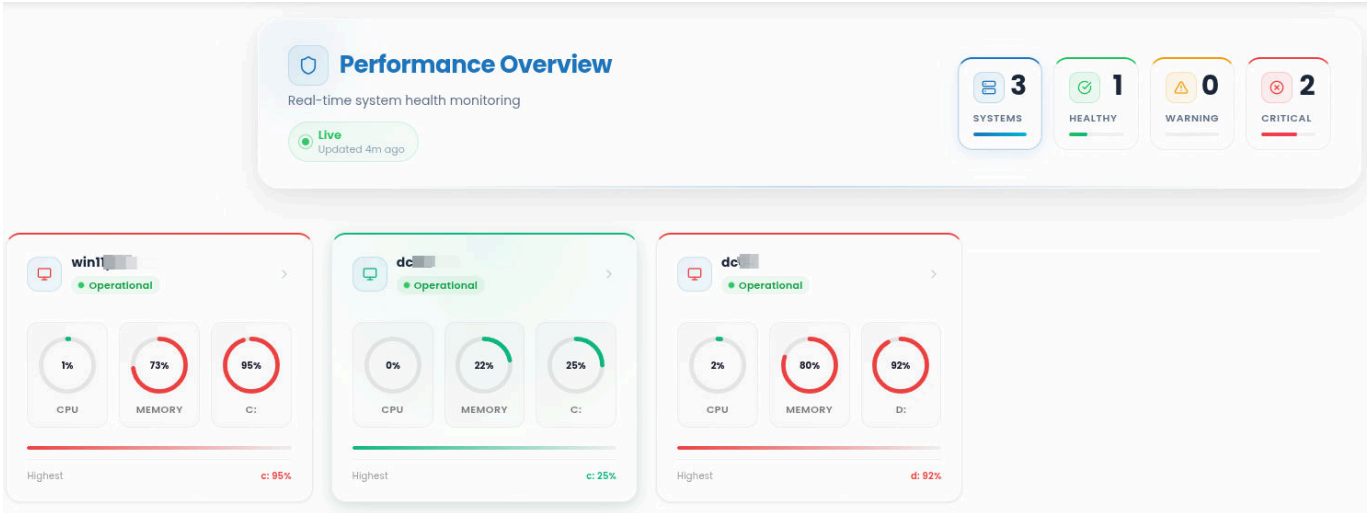
Performance Overview

The **Performance** module provides real-time system health monitoring for infrastructure components. It displays key resource usage indicators such as **CPU**, **memory**, and **disk utilization**, helping administrators quickly assess system status, detect abnormal resource consumption, and support troubleshooting or capacity planning activities.

The overview page displays the monitored systems as individual **system panels**. Each panel shows the current operational status, the latest CPU, memory, and disk usage values, and the highest resource usage indicator detected for that system.

At the top of the page, the **Performance Overview** panel summarizes the global health status of all monitored systems, including:

- **Systems** - Total number of monitored systems.
- **Healthy** - Systems currently operating within normal thresholds.
- **Warning** - Systems with resource usage approaching warning thresholds.
- **Critical** - Systems with resource usage exceeding critical thresholds.



Each monitored system panels includes the following metrics:

- **Last CPU** - Displays the latest CPU usage percentage for the monitored machine.
- **Last Memory** - Displays the latest RAM utilization percentage for the monitored machine.

- **Disk Usage** - Displays the latest disk usage percentage for the monitored machine.

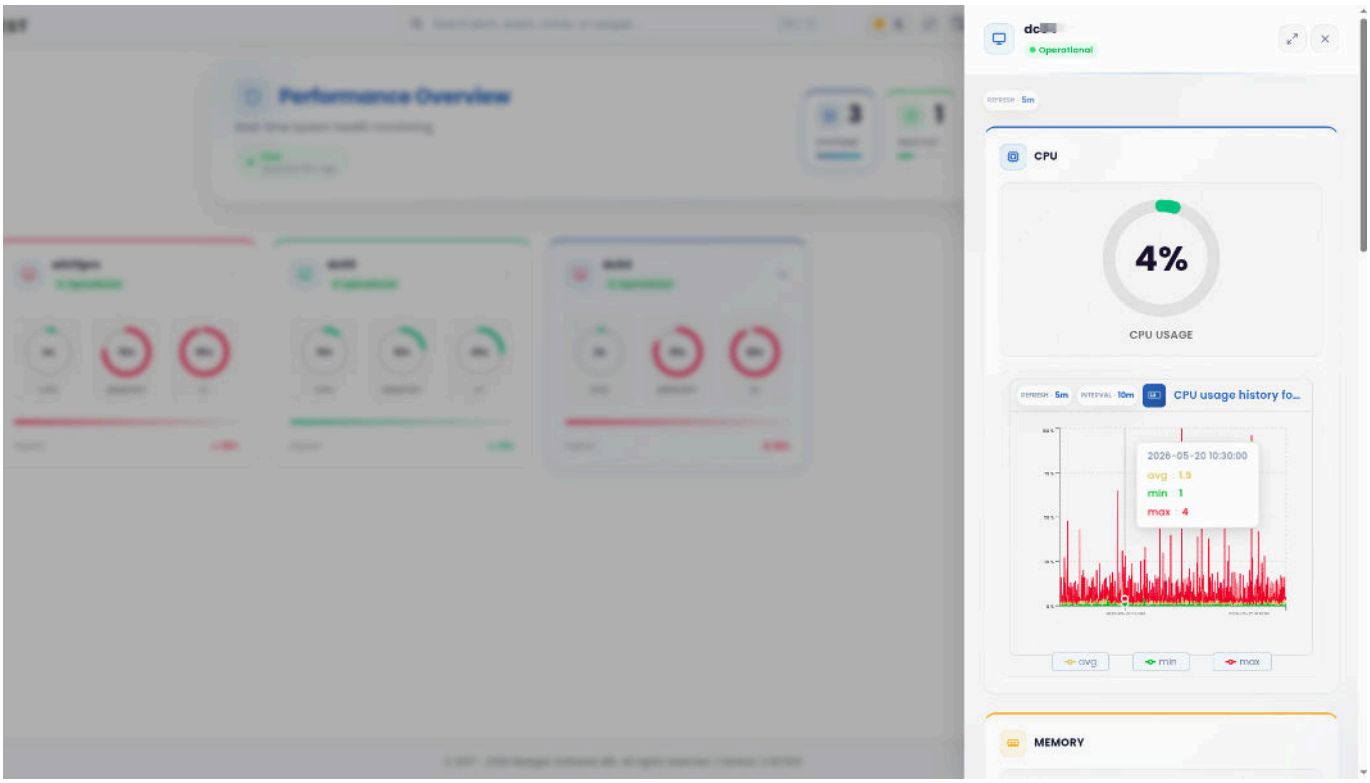
The colored status indicators help identify whether the system is operating normally or requires attention.

To open the detailed monitoring view for a system, click the

button on the system panel.

The detailed view displays expanded performance information for the selected system, including current usage values and historical charts for monitored resources. This view allows administrators to analyze resource behavior over time and identify usage spikes or performance trends.

Available refresh options may include **1 minute**, **5 minutes**, or **OFF**, depending on the selected metric and monitoring configuration.



To display the monitoring panel in a larger view, click the **Expand**

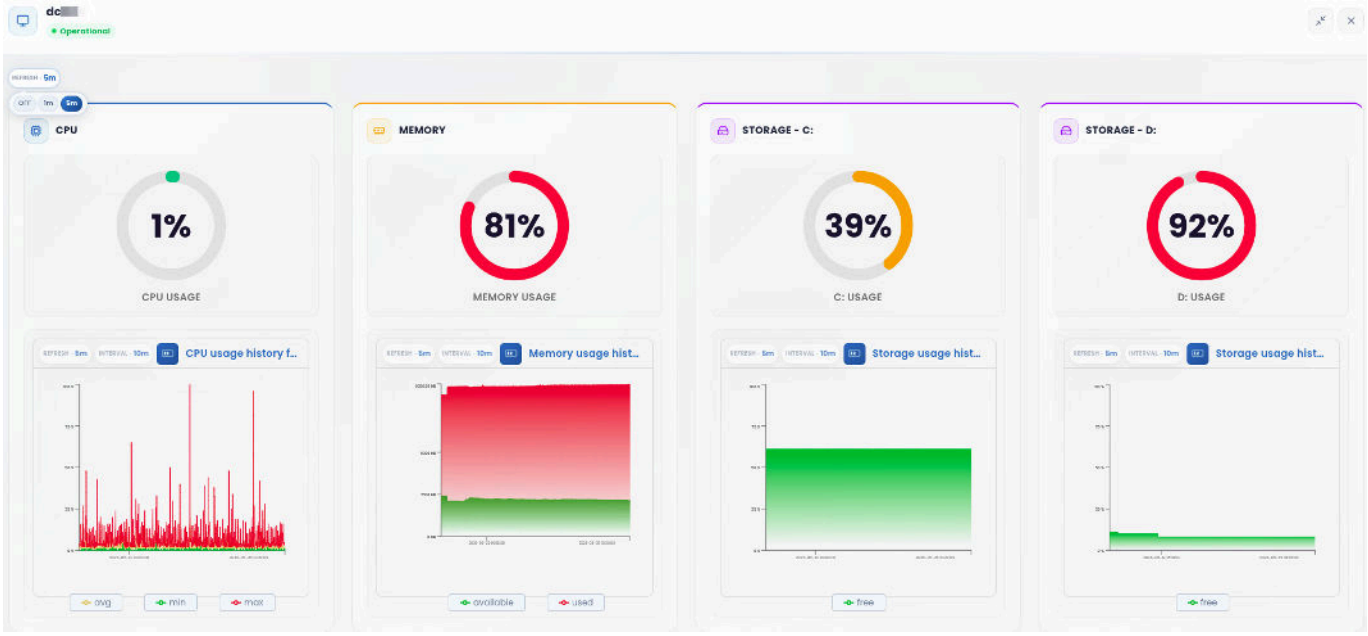


button.

System Performance Panels

The detailed system view displays dedicated performance panels for each monitored resource, such as **CPU**, **Memory**, and available **Storage drives**. Each panel provides the current usage value together with a historical chart, helping administrators analyze resource behavior over time.

The refresh interval can be configured to **1 minute**, **5 minutes**, or disabled by selecting **OFF**.



1. **CPU Panel**

The **CPU** panel displays the current processor usage for the selected system. The historical chart shows CPU usage over the selected time range and includes **average**, **minimum**, and **maximum** values. This helps administrators identify CPU spikes, abnormal load patterns, or sustained high usage.

2. **Memory Panel**

The **Memory** panel shows the current RAM utilization for the monitored system. The historical chart displays both **used memory** and **available memory** over the selected interval, allowing administrators to monitor memory pressure and identify possible resource exhaustion.

Available time intervals include **1m**, **10m**, **1h**, **6h**, **8h**, and **24h**, depending on the selected view.

3. **Storage Panels**

The **Storage** panels display disk usage for each monitored drive, such as **C:** or **D:**. Each panel shows the current usage percentage and a historical chart based on available or free storage capacity. This helps administrators track disk consumption trends and identify drives approaching critical usage levels.

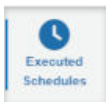
Each storage drive is displayed separately, allowing disk usage to be monitored individually for every available partition or volume.

Executed Schedules

This section displays reports that have been executed as part of scheduled tasks in the Reports Module. These are reports that were automatically generated based on predefined schedules rather than manual execution.

To access Executed Schedules:

1. Click the



icon in the left-side navigation menu of the Web Interface
2. The system will open the Executed Schedules page shown below:



For any of the executed reports schedules that are listed here, you can download or delete them.

- **Download** - Click the report's filename to initiate a ZIP archive download. Extract the archive to access the report in CSV format.
- **Delete** - Click the delete icon in the actions menu for the report. A confirmation dialog will appear to prevent accidental deletion:

For detailed instructions on creating scheduled reports, refer to the Scheduling Reports section in the Reports Module documentation.

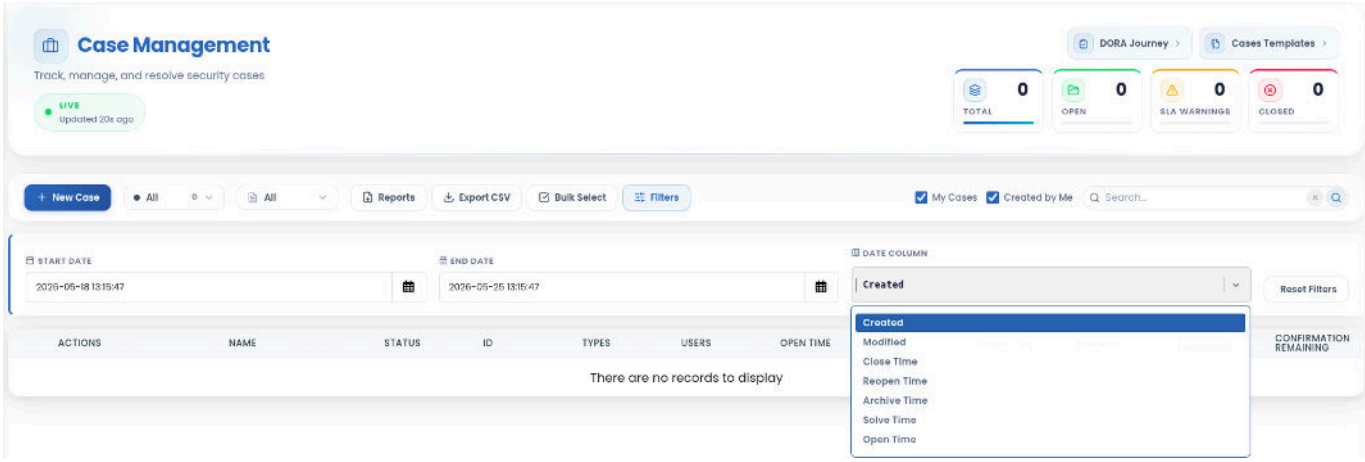
Case Management

CYBERQUEST provides a case management module designed to help organizations and users to create and track workflows in order to quickly address incidents. Every case created has an owner which can assign collaborators to enhance the decision-making process and streamline the case resolution. The case allows adding of all existing evidence based on the event or alert that led to creation of the case.

Overview

The **Case Management** module can be accessed by selecting "***Case Management***" button, in the left-side menu in Web Interface. The main interface presents a comprehensive view of all cases, offering intuitive controls for filtering, searching, and managing investigations.

Users are presented with **Case Management > My Cases** page allowing the managing of existing cases and opening new ones, as needed:



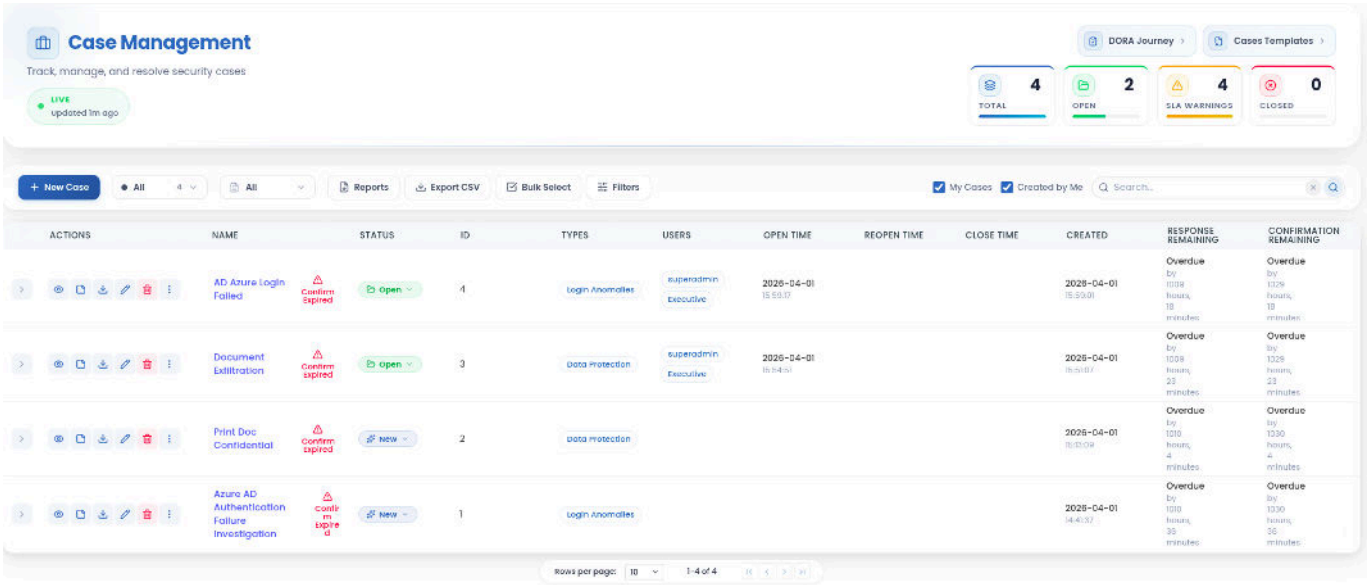
- To initiate a new investigation, click the **NEW CASE** button.
- To display all cases where the currently authenticated user is the owner, select the **My Cases** switch.

  To filter cases based on their status, use the Status drop-down menu. The available options include:

- **All:** Displays every case in the system, regardless of its current status.
- **New:** Shows recently created cases awaiting initial triage and assignment.

- **Open:** Lists active investigations currently being worked on by the security team.
- **Solved** - Displays cases marked as solved.
- **Closed** - Lists cases that have been finalized and closed.
- **Archived** - Shows cases that have been archived for record-keeping or future reference.
- **Template** - A drop-down list that allows selection of a predefined case template. These templates are created and managed in the *Case Templates* section and are used to streamline case creation
- To locate a specific case, use the **Quick Filter** search box available on the right side of the web interface.
- All cases are displayed in chronological order, with the most recently created cases appearing at the top of the list.

In the case list, the **Actions** menu is located on the right side and provides options to **view**, **export**, **edit**, or **delete** a case.



To remove a case, click the



button located in the top-right corner of the Case Management interface.

To modify a selected case, click the



button in the same area.

Use the



button to export case data.

The **Response Remaining / Confirm Remaining** columns provide critical visibility into service level agreement (SLA) compliance, ensuring timely incident response and resolution. These metrics help security teams prioritize cases and meet regulatory requirements.

- **Response Due Time:** Indicates the deadline for initial case acknowledgment and assignment. This is the time by which the security team must acknowledge the case and begin initial investigation.
- **Confirmation Due Time:** Represents the deadline for confirming the resolution of the case. This is the time by which the security team must confirm that all necessary remediation steps have been taken and the incident is fully resolved.

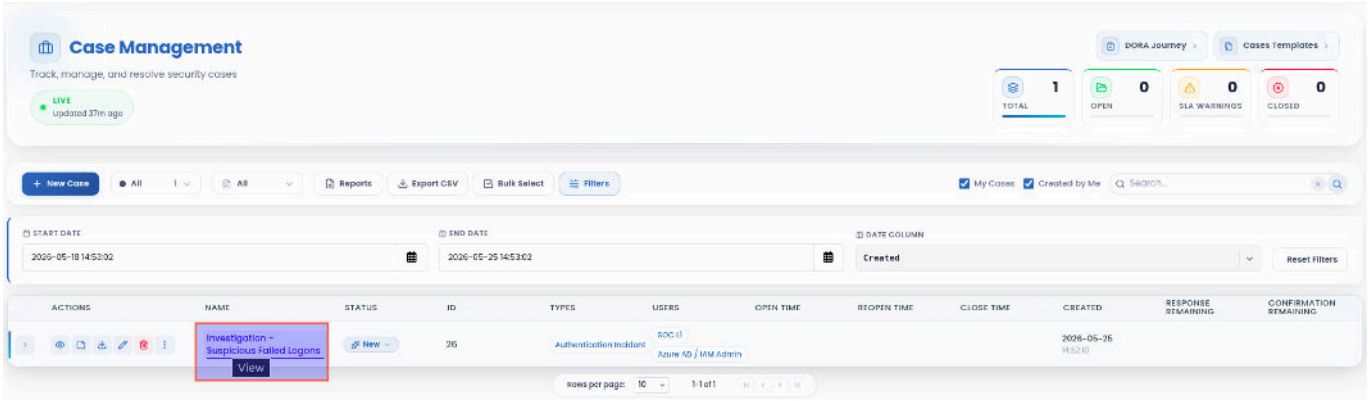
- **Response Remaining:** Shows the time remaining until the Response Due Time is reached. If this time has passed, it indicates how much time has elapsed since the deadline was missed.
- **Confirm Remaining:** Shows the time remaining until the Confirmation Due Time is reached. If this time has passed, it indicates how much time has elapsed since the deadline was missed.

Detailed Case View

The **Case Details View** presents essential information and metadata related to a specific case. This includes general identifiers such as **Case ID**, name, type, and description, along with timestamps marking important lifecycle events - like when the case was created, modified, closed, or reopened.

It also provides SLA-related metrics such as **Response Due Time**, **Confirmation Due Time**, and their respective remaining or overdue durations. Ownership and access are indicated by fields like **Case Owner**, assigned users, and current **Status**.

Additional insights include duplication tracking (e.g., duplication hash and count), user classification, and whether the case is flagged as a duplicate or the most recent duplicate. These details support efficient case management, auditing, and prioritization.



Click the

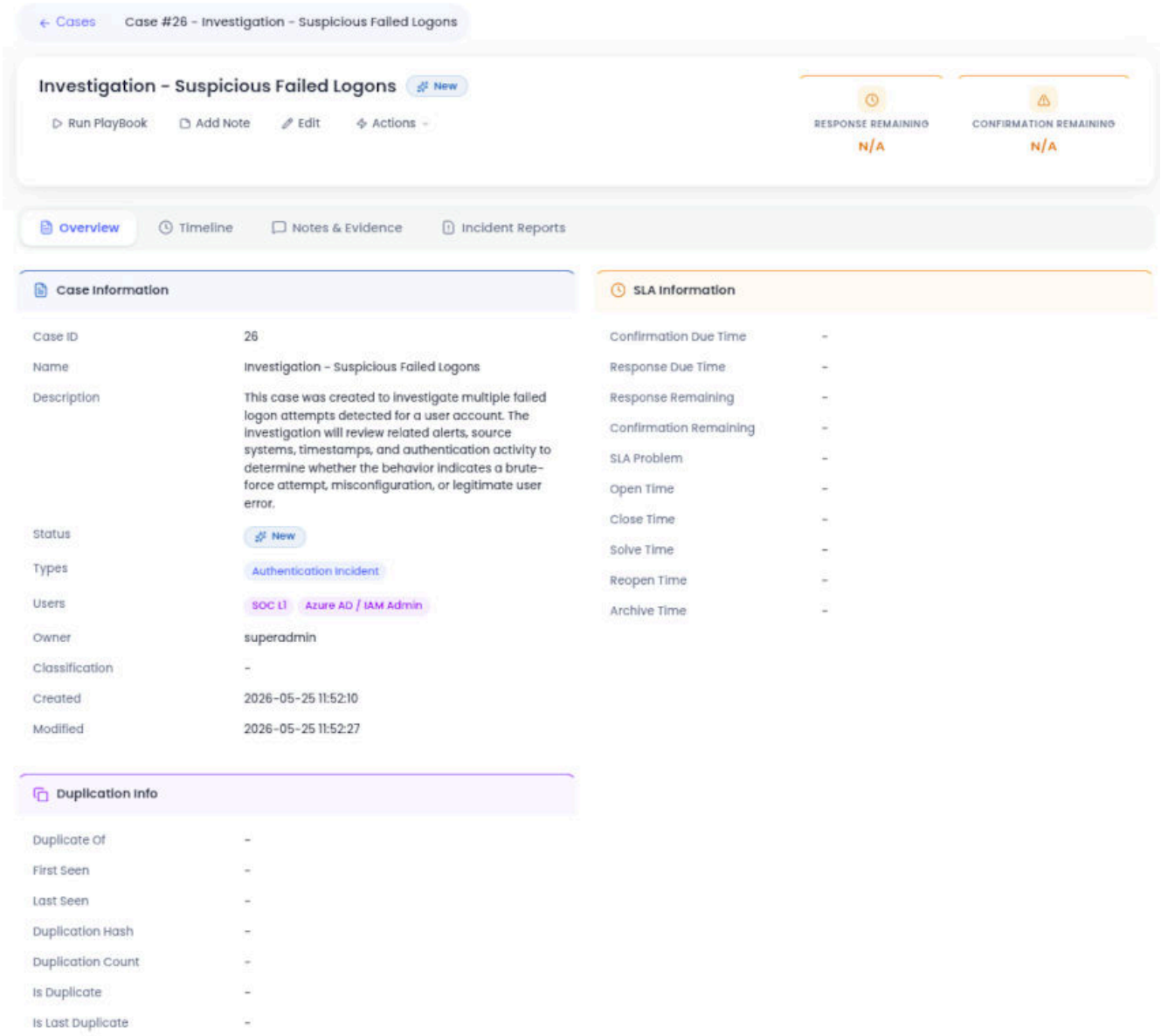


button to open a quick view of a specific case. Alternatively, click the case name to access the case details:

The case details page is organized into several views:

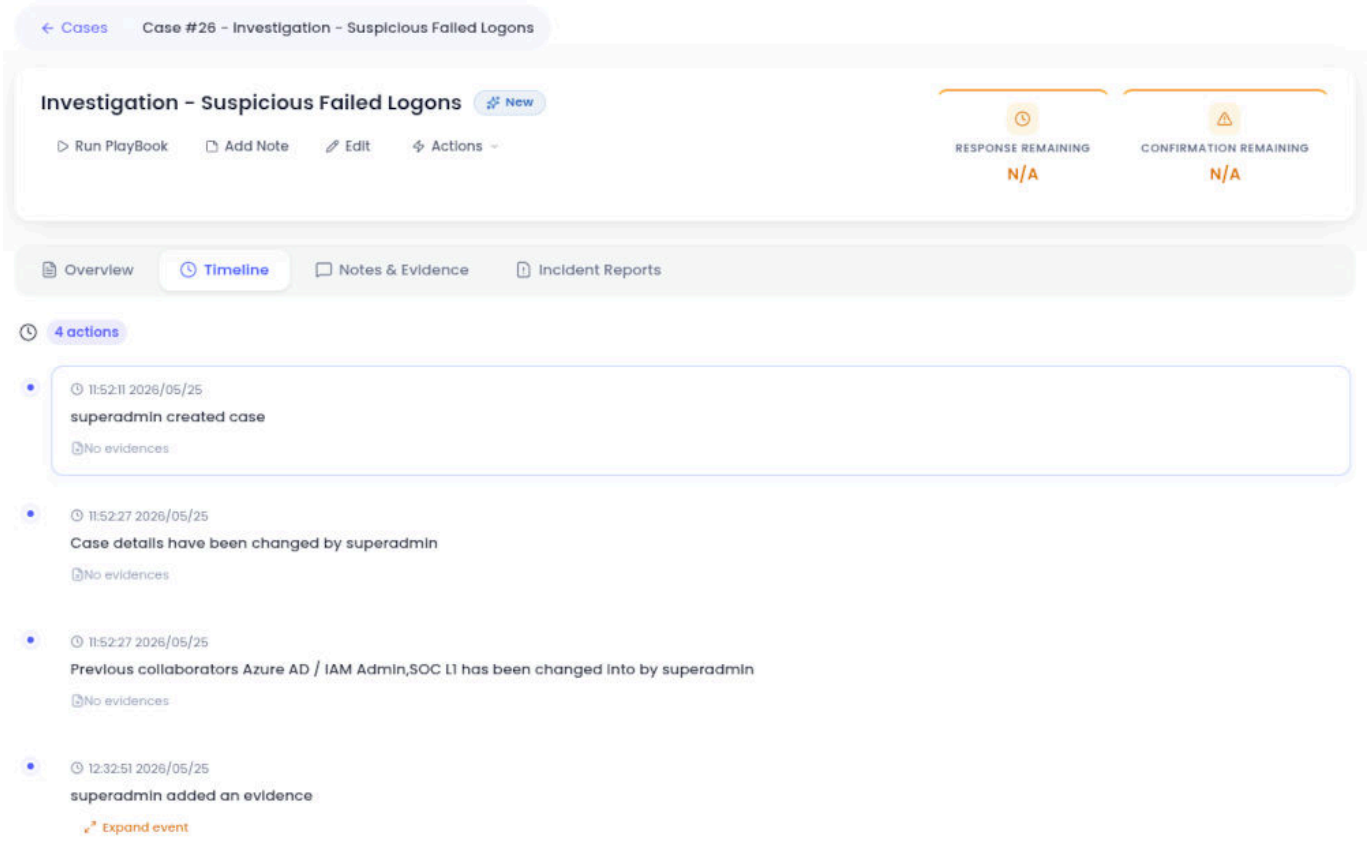
Overview

The **Overview** tab displays the main information about the selected case, including case ID, name, description, status, type, assigned users, owner, creation date, and last modification date. It also includes SLA and duplication information, helping users quickly understand the current state and context of the case.



Timeline

The **Timeline** tab provides a chronological history of all actions performed on the case. It helps users track case activity, such as creation, updates, collaborator changes, and evidence additions.

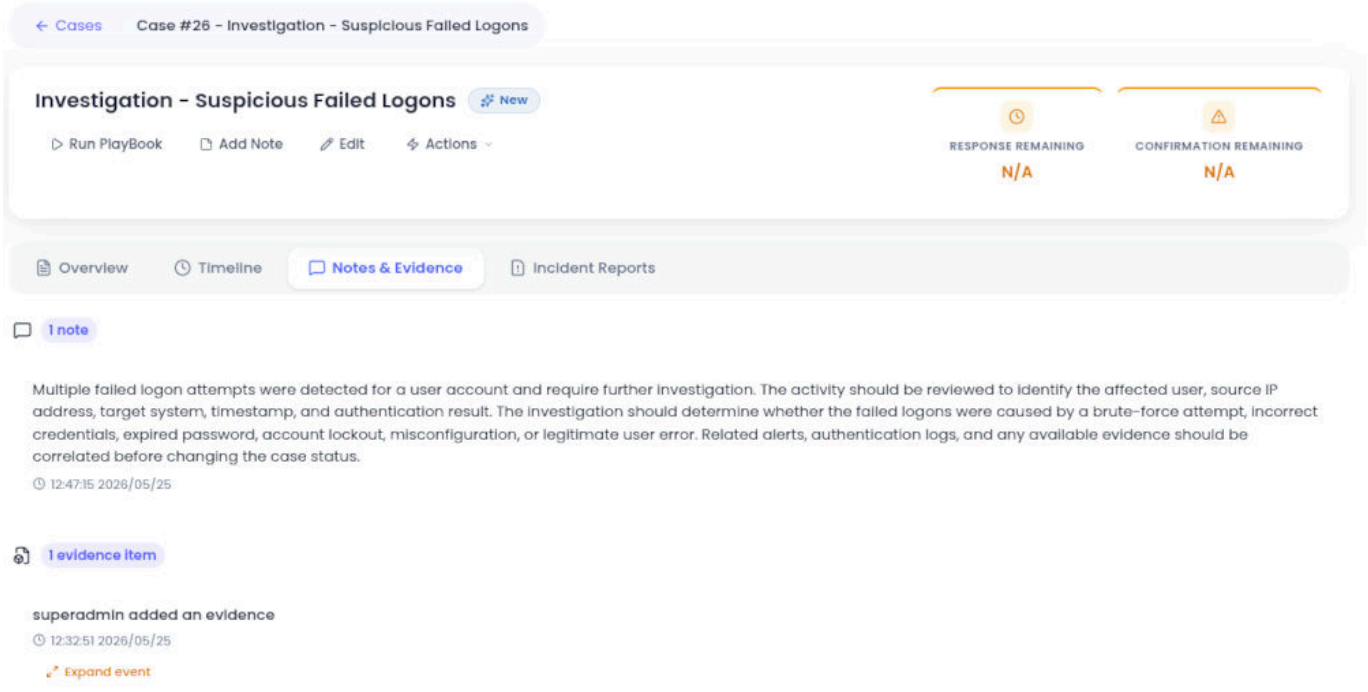


Notes & Evidence

The **Notes & Evidence** tab displays notes and evidence items associated with the case.

The **Notes** area shows comments or investigation notes added by users. If no notes are available, the interface displays a no-notes message.

The **Evidence** area lists uploaded or attached evidence items, such as logs, screenshots, exported alerts, or other supporting files. Evidence entries include the user who added the item and the timestamp. The user can expand the evidence entry to review additional information.

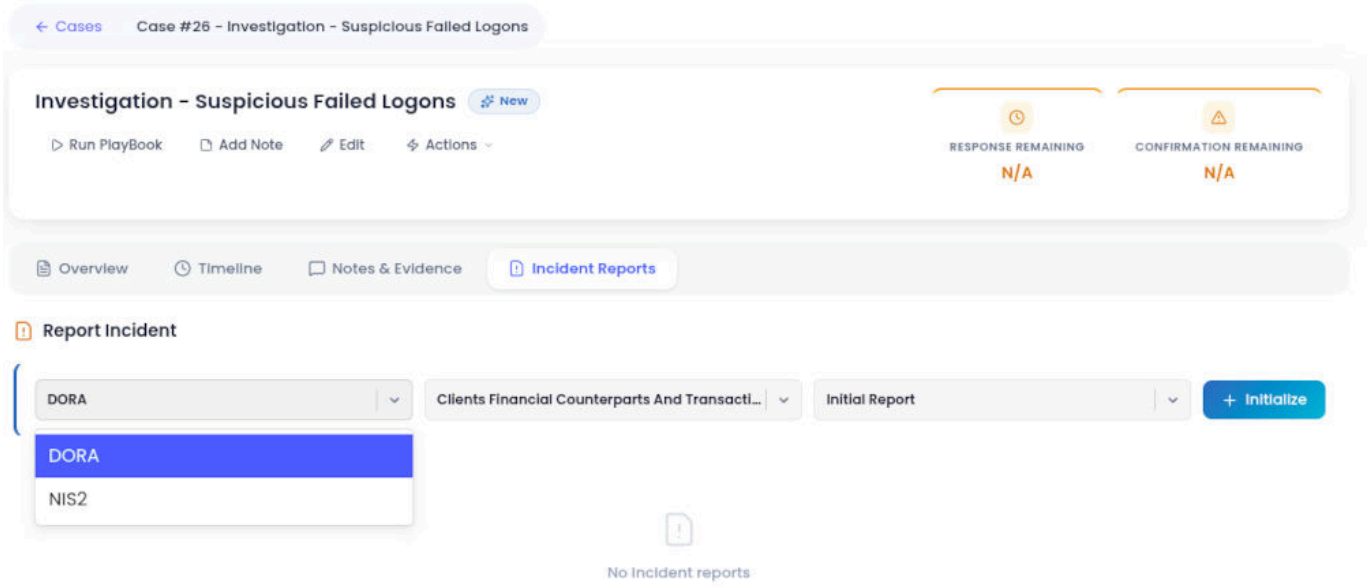


Incident Reports

The **Incident Reports** tab allows users to initialize and manage incident reports associated with the case.

From this view, the user can select the reporting framework, such as **DORA** or **NIS2**, choose the relevant incident report category, select the report type, and initialize the report.

This section is used to support regulatory reporting workflows by linking incident documentation directly to the investigation case. If no reports have been created, the interface displays a no incident reports message.



At the top of the page, available actions include *running a playbook*, *adding a note*, *editing the case*, and *changing the case status*.

Cases Manual Deduplication

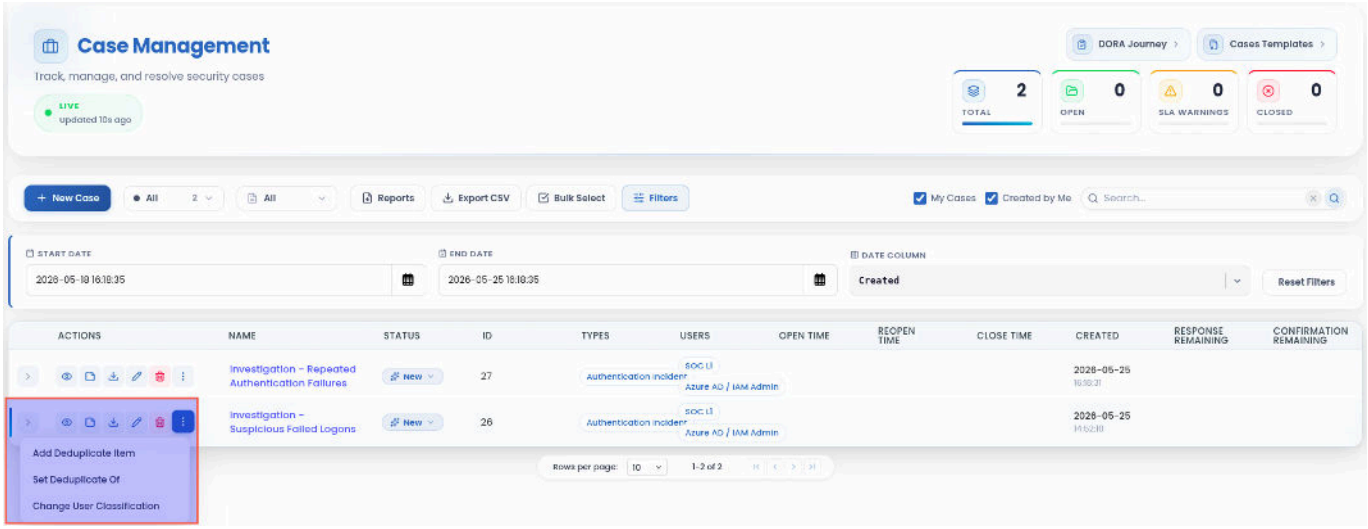
Manual deduplication allows analysts to link cases that are determined to be related or identical based on their investigation. This process streamlines case management, reduces redundancy, and ensures that all relevant information is consolidated under the most appropriate case.

To start manual deduplication, click the

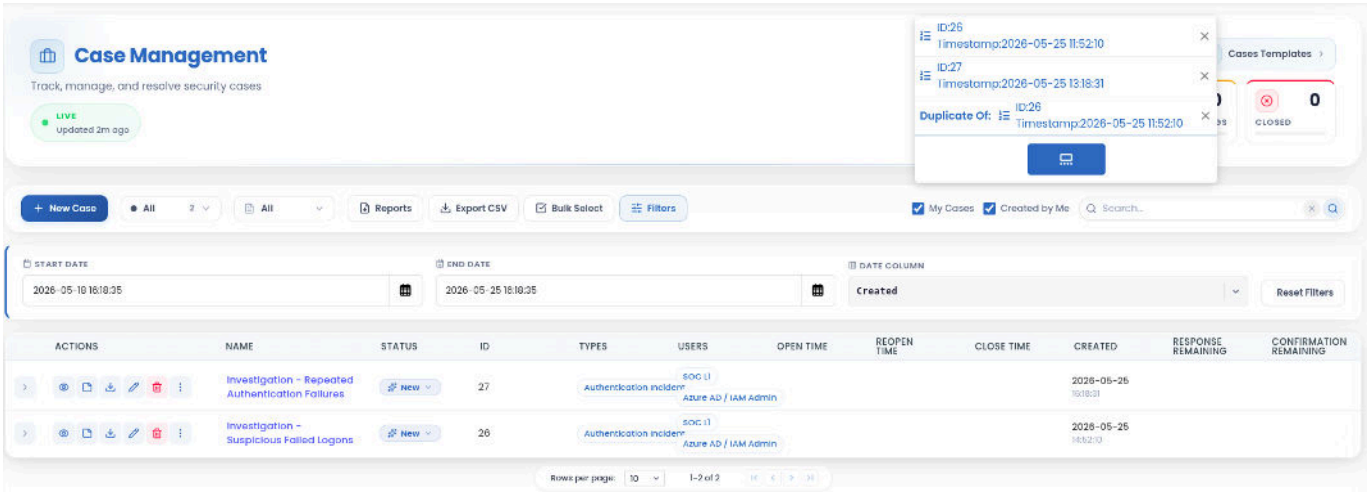


button. From the actions menu, select **Add Deduplicate Item**.

After the case is added as a deduplication item, open the actions menu again and select **Set Deduplicate Of**. This option allows the user to choose the primary case that the current case will be linked to as a duplicate.



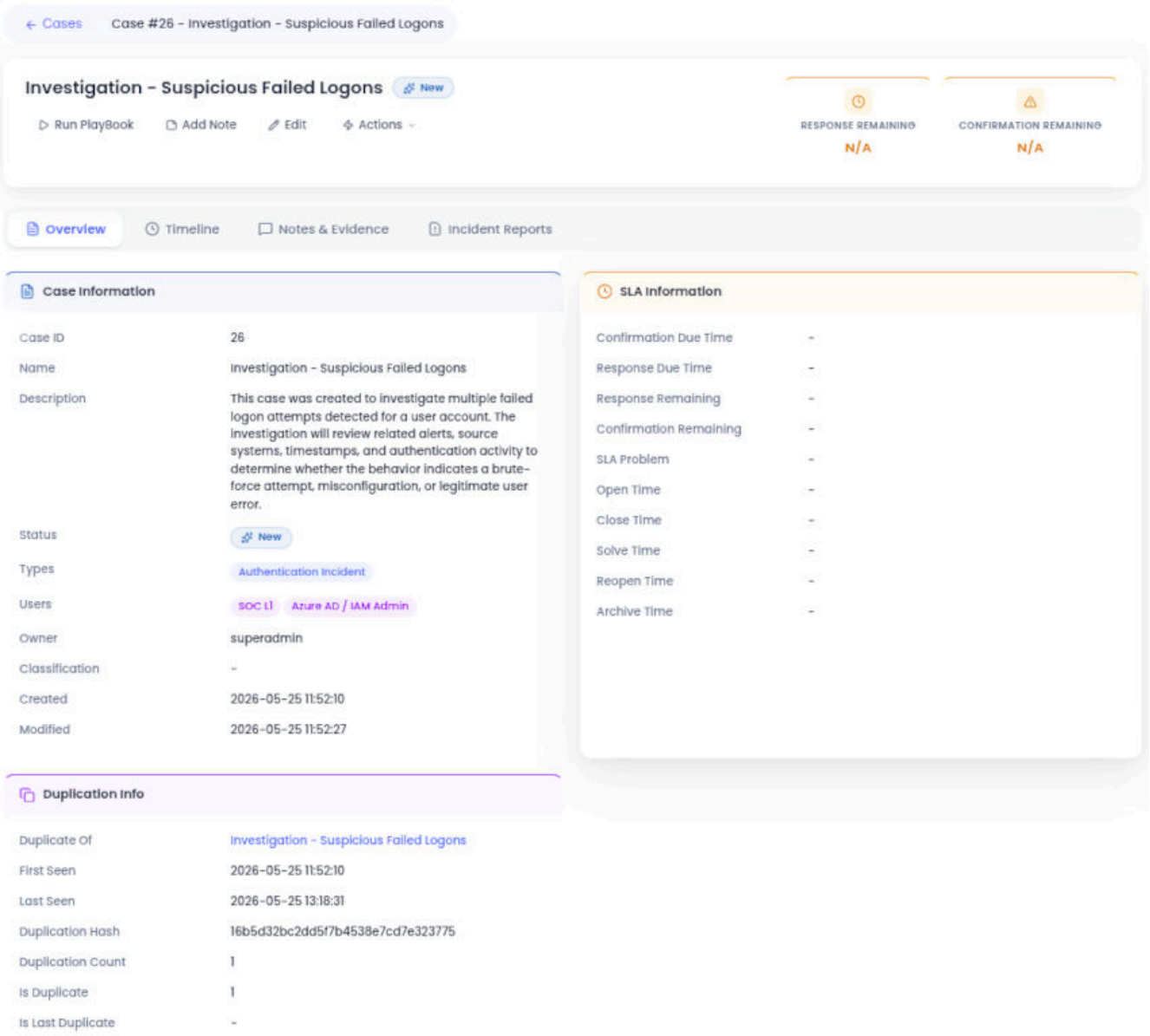
In the deduplication selection window, review the selected cases and the **Duplicate Of** relationship. After confirming the selection, click the confirmation button to apply the deduplication relationship.



Deduplication Options:

- **Add Deduplicate Item:** Adds the current case to a temporary list of items that are considered potential duplicates. This list is used to build a set of related cases before assigning a primary case.
- **Set Deduplicate Of:** Assigns the current case as a duplicate of another case selected from the list previously built using **Add Deduplicate Item**. This action establishes a clear relationship between the duplicate case and the primary case, consolidating all relevant information under the primary case.

  Once the deduplication is applied, the relationship is displayed in the **Duplication Info** section of the case details view.



The **Duplication Info** section displays details about the deduplication relationship, including the primary case, first seen and last seen timestamps, duplication hash, duplication count, and whether the current case is marked as a duplicate.

For example, if **Investigation - Repeated Authentication Failures** refers to the same activity as **Investigation - Suspicious Failed Logons**, the analyst can add the repeated authentication case as a deduplication item and then set it as duplicate of the suspicious failed logons case.

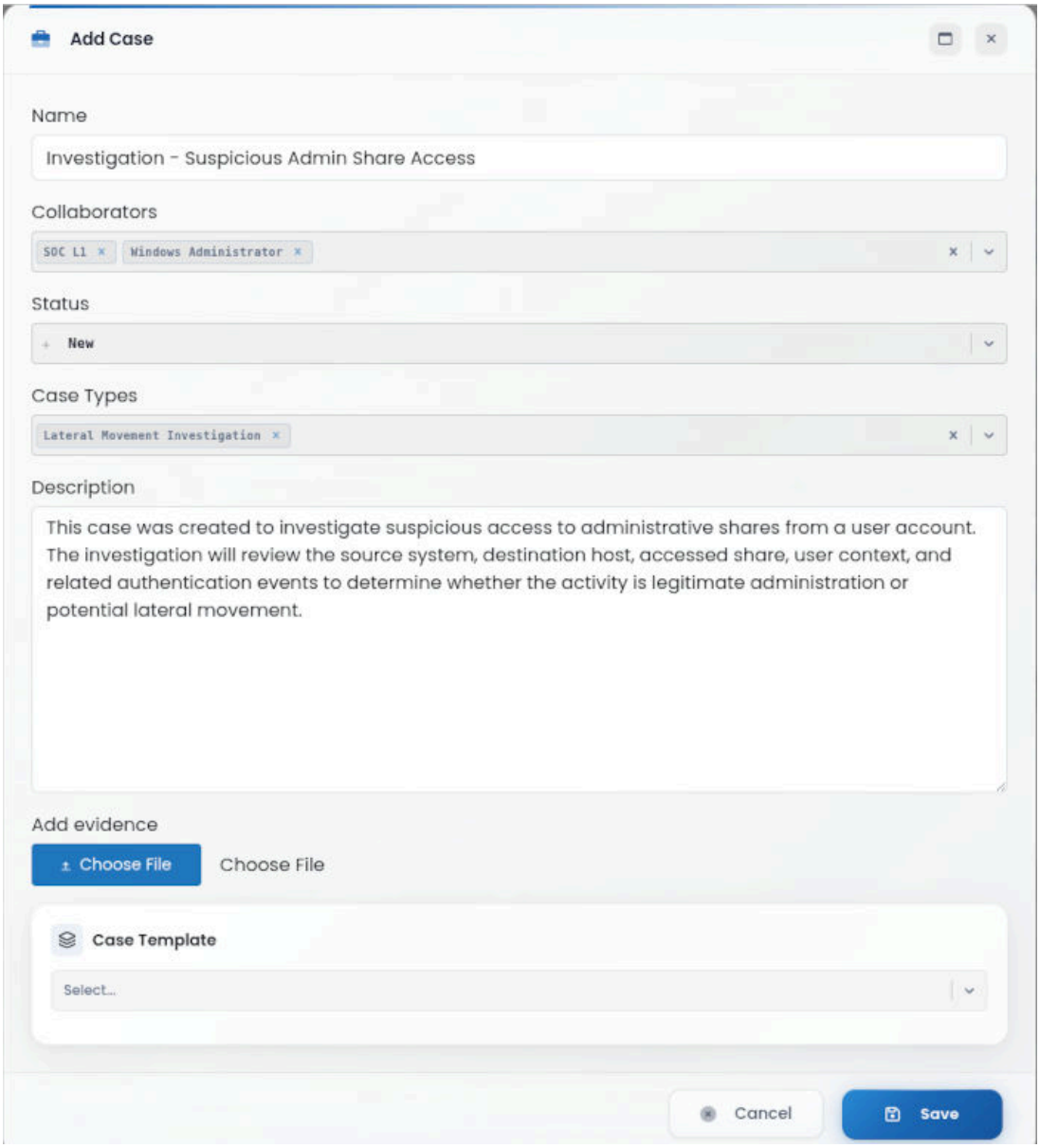
Create a New Case

The **Case Management** module allows users to create investigation records that group related alerts, evidence, notes, and user activity into a structured workflow. Each case acts as a central workspace for tracking investigation progress, assigning responsibilities, documenting findings, and maintaining a clear audit trail throughout the incident lifecycle.

To create a new case, click the



button. This opens the case creation window.



The following fields can be configured:

- **Name:** Enter a clear and descriptive case title that reflects the issue being investigated. Using a consistent naming convention helps improve traceability and makes cases easier to identify later.
- **Collaborators:** Select the users who will participate in the investigation or require access to the case. Collaborators can review case details, add notes, upload evidence, and contribute to the investigation process.
- **Status:** Select the current phase of the case from the dropdown menu:
  - `New` - The case has been created and is awaiting initial review or triage.
  - `Open` - The case is actively being investigated by the security team.
  - `Solved` - The issue has been resolved, but the case may still require final validation or documentation.
  - `Closed` - The case has been completed and no further action is required.
  - `Archived` - The case has been retained for historical, audit, or compliance purposes.

  It is recommended that each organization defines an internal procedure for when cases should move between statuses such as **New**, **Open**, **Solved**, **Closed**, and **Archived**.
- **Case Types:** Select the category that best describes the investigation. Case types help organize, filter, and analyze cases based on the nature of the incident.

- **Description:** Provide a short explanation of the case context, including why the case was created, what activity is being investigated, and what the expected analysis should cover.
- **Evidence:** Upload supporting files related to the case, such as logs, screenshots, exported alerts, reports, or other relevant investigation materials.
- **Case Template:** Select a predefined template to standardize the case structure. Templates are managed in the **Case Templates** section and help reduce manual effort when creating recurring or similar investigation cases.

Click the **"Save"** button to apply the changes and create the case, or select **"Cancel"** to discard and return to the main page.

Edit Case

To modify an existing case, click the



button. The **Edit Case** window allows updates to key case details like as title, status, description, collaborators, attached evidence, and case template. After making the necessary changes, click **"Save"** to confirm or **"Cancel"** to discard and return to the main page.

Attach a Ticket

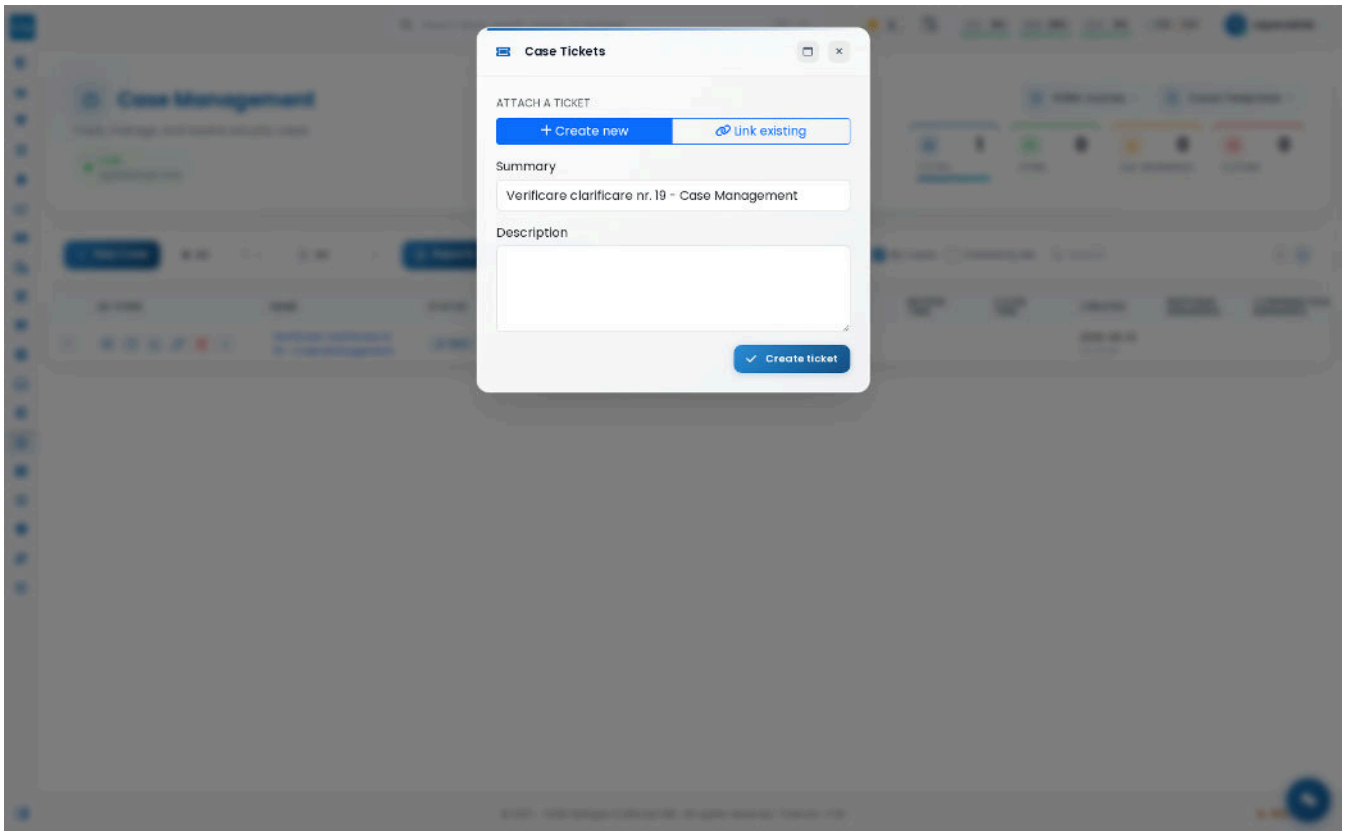
A case can be linked to a ticket in an external ticketing system directly from the case list, without leaving the **Case Management** module. This requires a ticketing provider to be configured under **Settings → Ticketing**.

To attach a ticket, click the

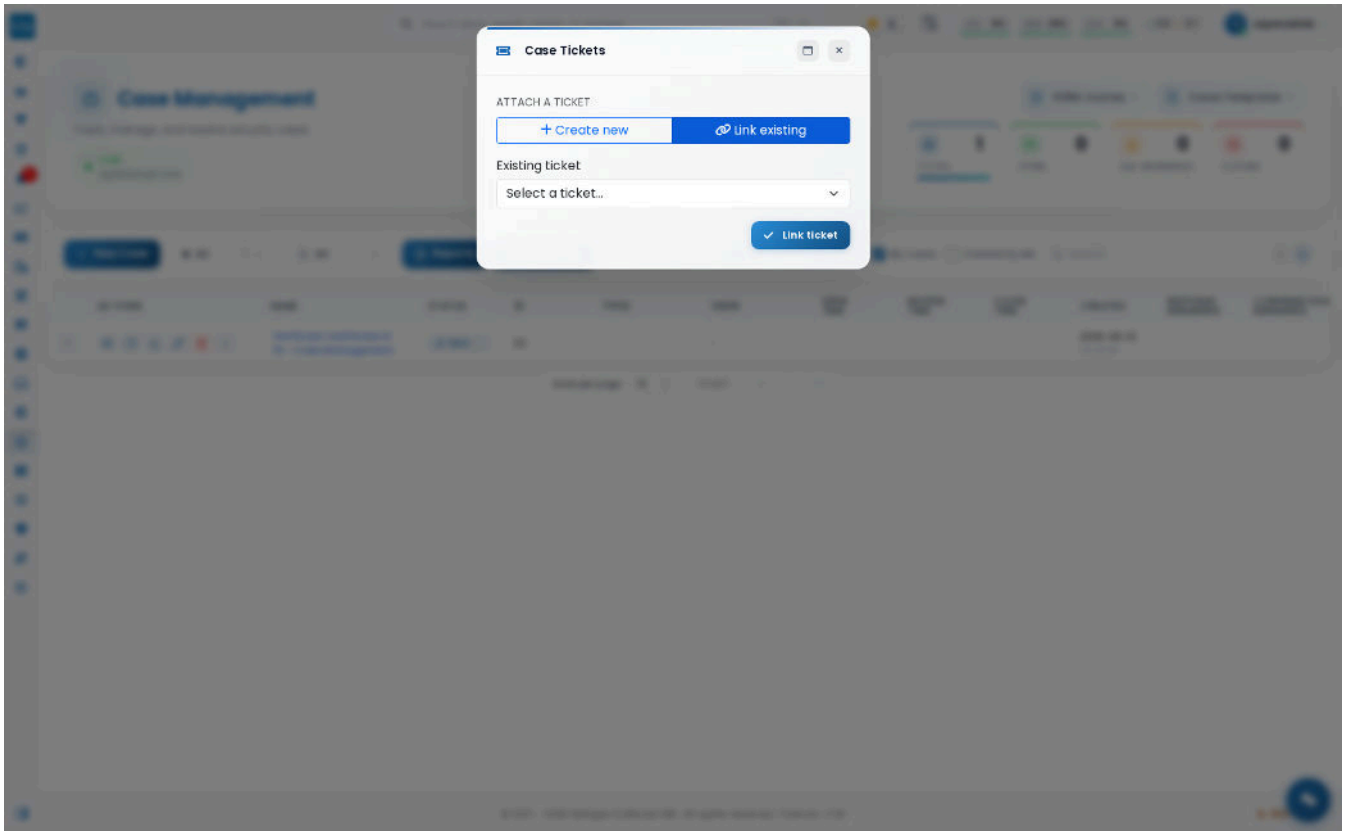


button on the case row and select **Attach ticket**. The **Case Tickets** window opens with two modes:

- **Create new** - Creates a brand new ticket in the configured external ticketing system. The **Summary** and **Description** fields are pre-filled from the case name and description, and can be edited before the ticket is created.



- **Link existing** - Links the case to a ticket that already exists in the external system. The **Existing ticket** drop-down is populated live, by querying the configured provider for open tickets, so the list always reflects the current state of the external system rather than a cached snapshot.



Once a ticket is attached, it appears in the **Attached tickets** list with a link to open it directly in the external system. A ticket can be detached from the case at any time using the **Unlink** action next to it, without affecting the ticket in the external system.

Generate Reports

The **Generate Reports** feature allows users to export case information from the **Case Management** module for documentation, review, audit, or compliance purposes. Reports are generated in **HTML format** and can include either a general case overview or a more detailed report based on selected case data tables.

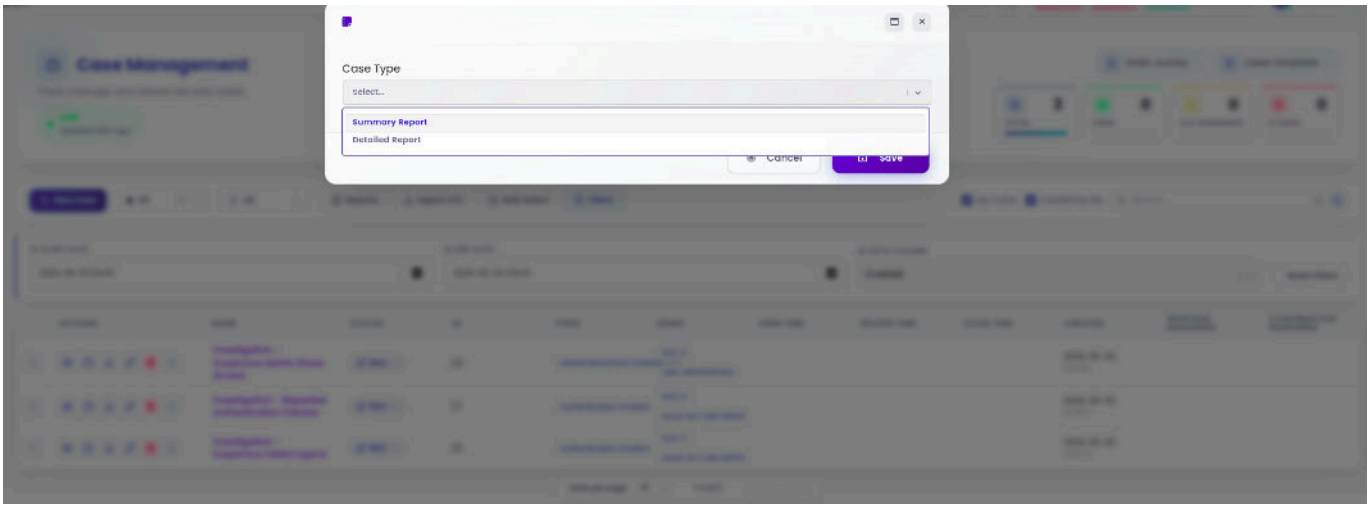
To generate a report, click the



button from the **Case Management** toolbar. This opens the report generation window.

The following report types are available:

- **Summary Report** - Generates a general overview of the cases available in **Case Management**. This report includes high-level statistics such as the total number of cases, closed cases, close time values, total investigation time, and generation details.



CYBERQUEST

Cases overview

Start date: 2026-05-19 11:16:10
End date: 2026-05-26 11:16:10

Total number of cases	3
Total number of closed cases	1
Minimum close time (minutes)	37
Maximum close time (minutes)	37
Average close time (minutes)	37
Total investigation time (minutes)	37

Generated at: 2026-05-26 08:53:19
Generated by: superadmin

- **Detailed Report** - Allows the user to generate a customized case report by selecting specific tables from the available list. This option is useful when the report must include only certain categories of case information.

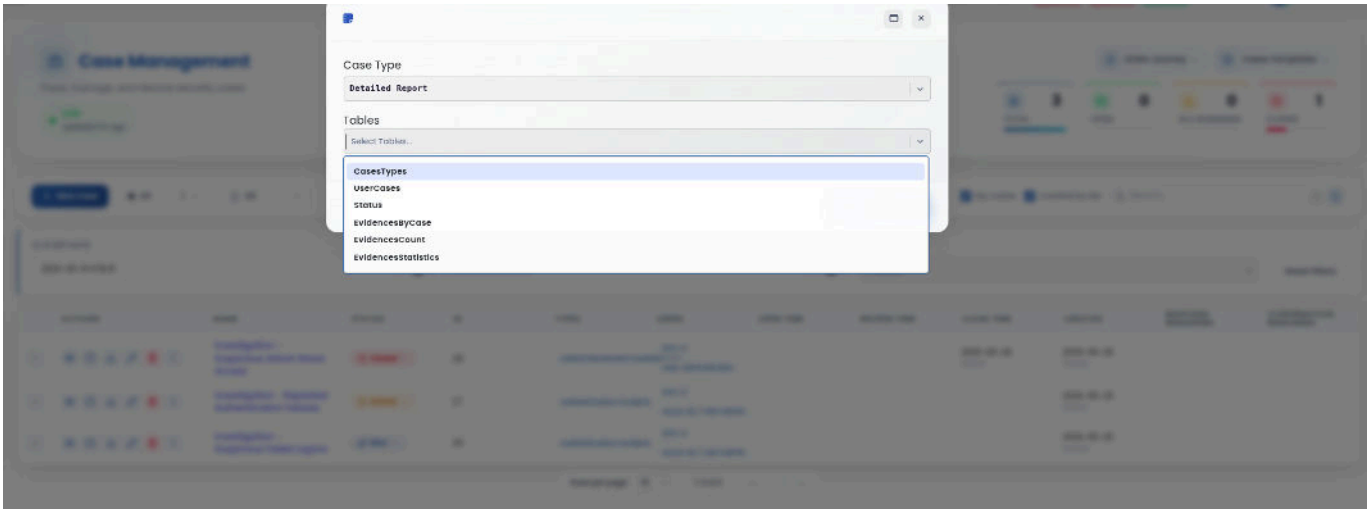
  When **Detailed Report** is selected, the **Tables** field becomes available. From this drop-down list, users can choose the information that should be included in the exported report.

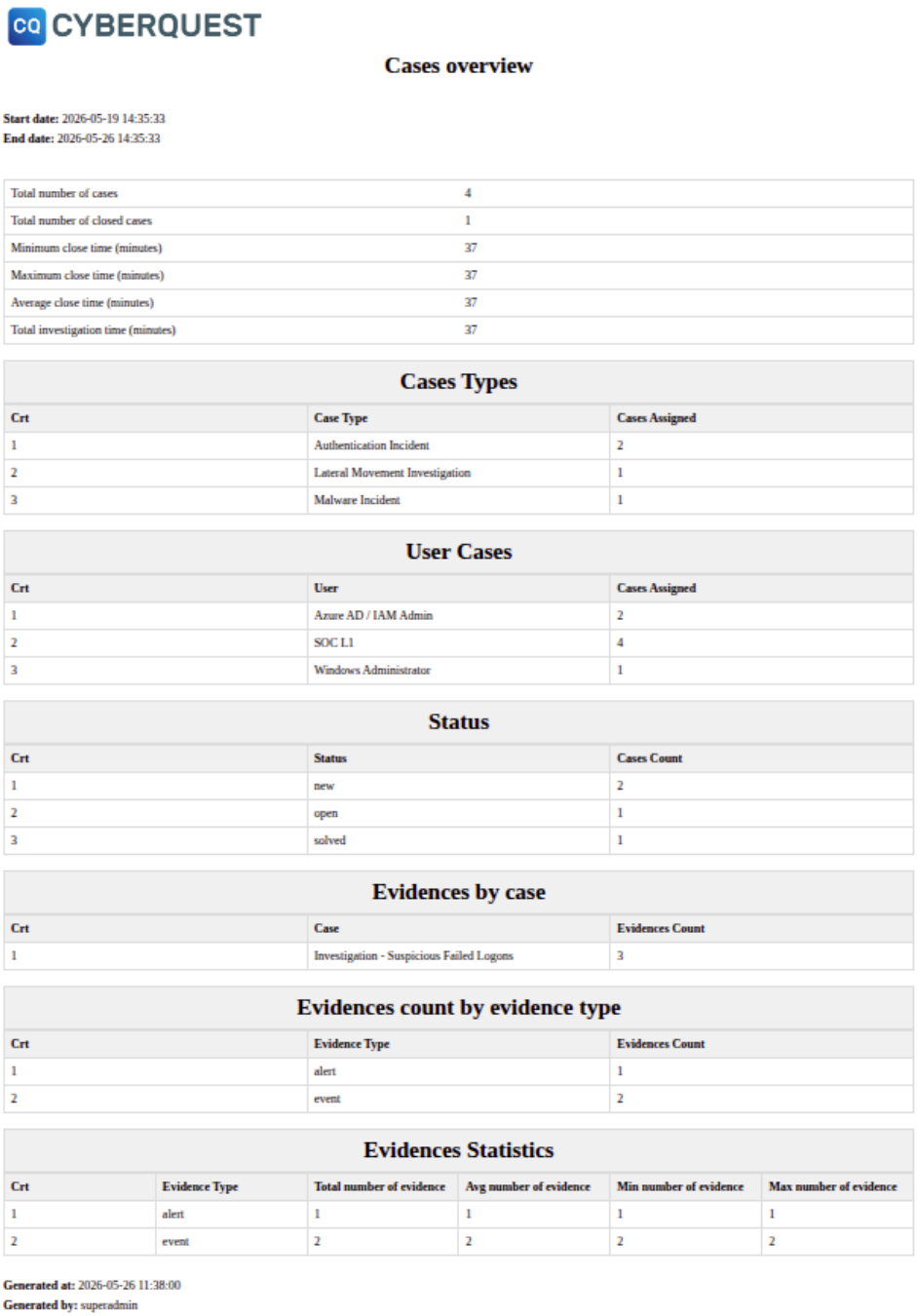
  Available tables may include:

  - **CasesTypes** - Displays case distribution by case type.

- **UserCases** - Displays the number of cases assigned to each user.
- **Status** - Displays case count grouped by status.
- **EvidencesByCase** - Displays the number of evidence items linked to each case.
- **EvidencesCount** - Displays evidence count grouped by evidence type.
- **EvidencesStatistics** - Displays evidence-related statistics, such as total, average, minimum, and maximum evidence count.

After selecting the report type and the required tables, click **Save** to generate the report. The exported HTML file can then be used for internal documentation, investigation review, management reporting, or audit evidence.





CYBERQUEST

Cases overview

Start date: 2026-05-19 14:35:33
End date: 2026-05-26 14:35:33

Total number of cases	4
Total number of closed cases	1
Minimum close time (minutes)	37
Maximum close time (minutes)	37
Average close time (minutes)	37
Total investigation time (minutes)	37

Cases Types

Crt	Case Type	Cases Assigned
1	Authentication Incident	2
2	Lateral Movement Investigation	1
3	Malware Incident	1

User Cases

Crt	User	Cases Assigned
1	Azure AD / IAM Admin	2
2	SOC L1	4
3	Windows Administrator	1

Status

Crt	Status	Cases Count
1	new	2
2	open	1
3	solved	1

Evidences by case

Crt	Case	Evidences Count
1	Investigation - Suspicious Failed Logons	3

Evidences count by evidence type

Crt	Evidence Type	Evidences Count
1	alert	1
2	event	2

Evidences Statistics

Crt	Evidence Type	Total number of evidence	Avg number of evidence	Min number of evidence	Max number of evidence
1	alert	1	1	1	1
2	event	2	2	2	2

Generated at: 2026-05-26 11:38:00
Generated by: superadmin

Associating Events/Alerts with a Case

Case Management is tightly integrated throughout key CYBERQUEST investigation modules, enabling seamless transition from threat identification to investigation. This integration allows security analysts to efficiently convert potential security incidents identified in other modules directly into managed cases. Wherever the **Case Management** action menu is available - typically accessible via an action arrow - items can be used as evidence by creating a new case or attaching them to an existing one.

Integration with Browser Module

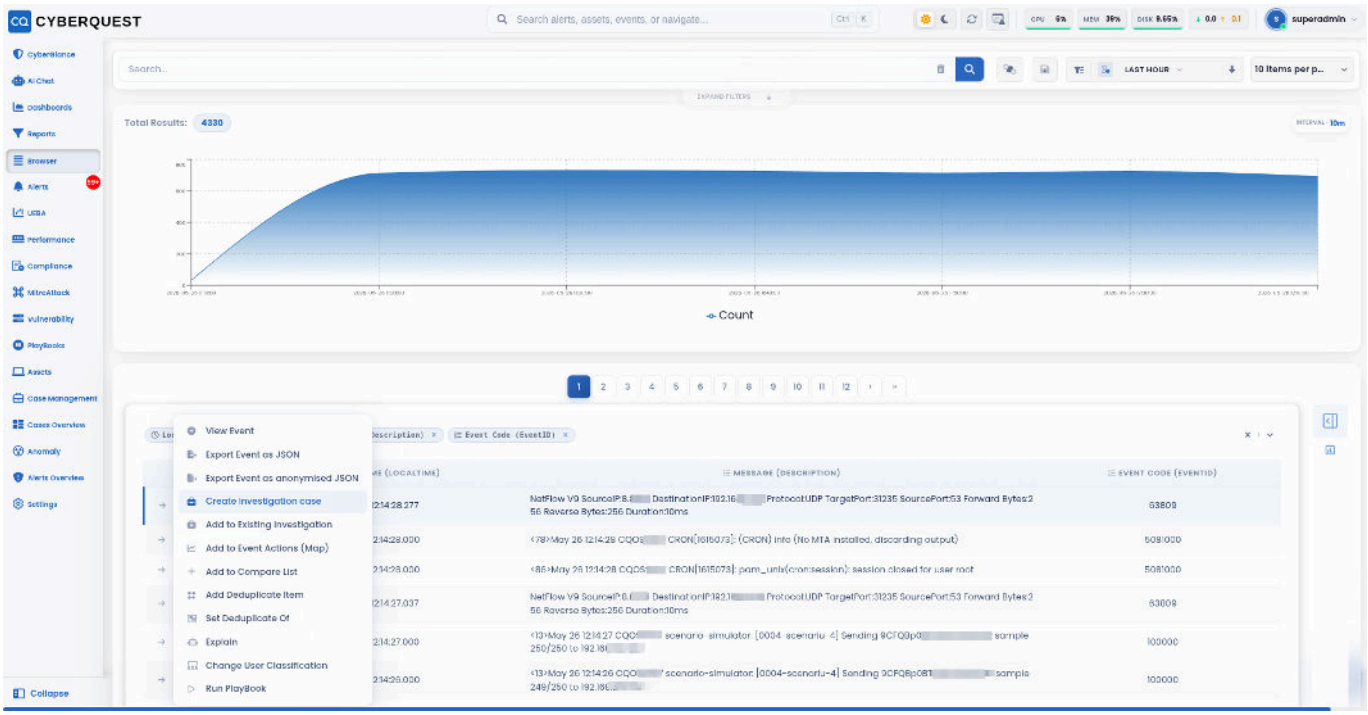
The **Browser** module allows users to review, filter, and analyze security events in detail. When an analyst identifies an event that requires further investigation, the event can be used to create a new investigation case or can be added as evidence to an existing case.

To create or update an investigation case from the **Browser** module:

1. Navigate to the **Browser** module and locate the event that requires investigation.
2. Click the

icon next to the selected event to open the event actions menu.

3. From the actions menu, select one of the following options:
   - **Create Investigation Case** - Opens a new case creation window and automatically adds the selected event as evidence for the new case.
   - **Add to Existing Investigation** - Allows the user to select an existing case and attach the selected event as evidence to that investigation.



Integration with Alerts Module

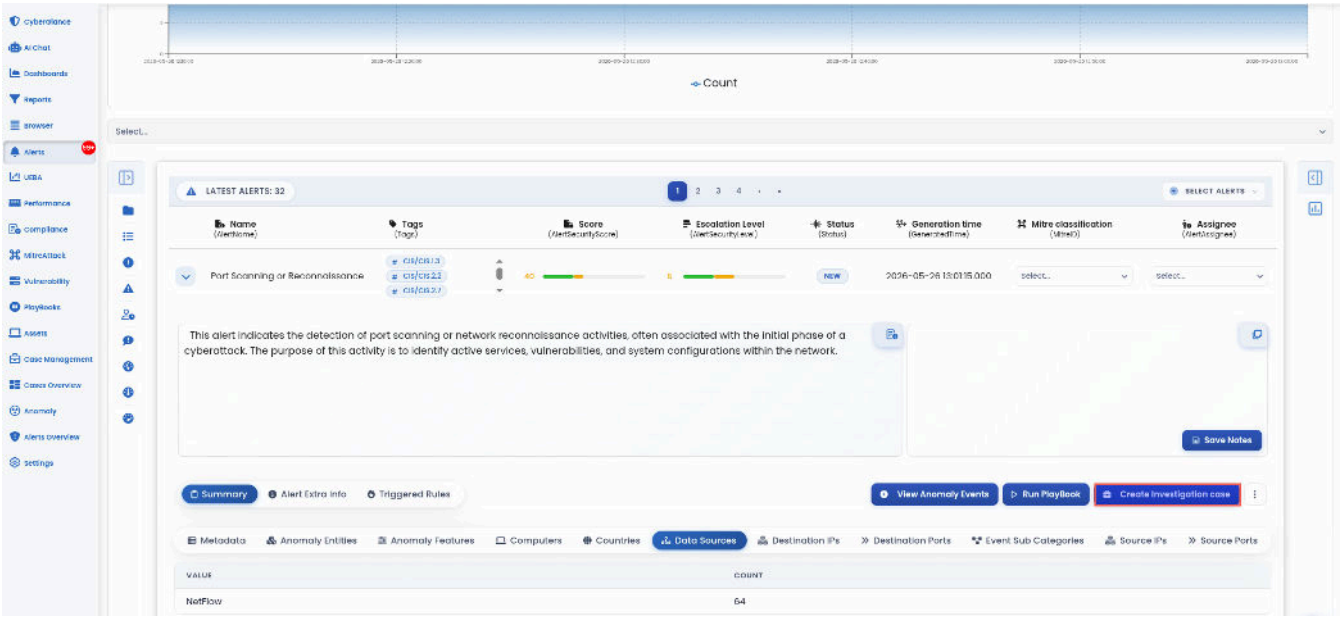
The **Alerts** module allows analysts to create or update investigation cases directly from detected alerts. When an alert requires further analysis, it can be converted into a new case or attached as evidence to an existing investigation.

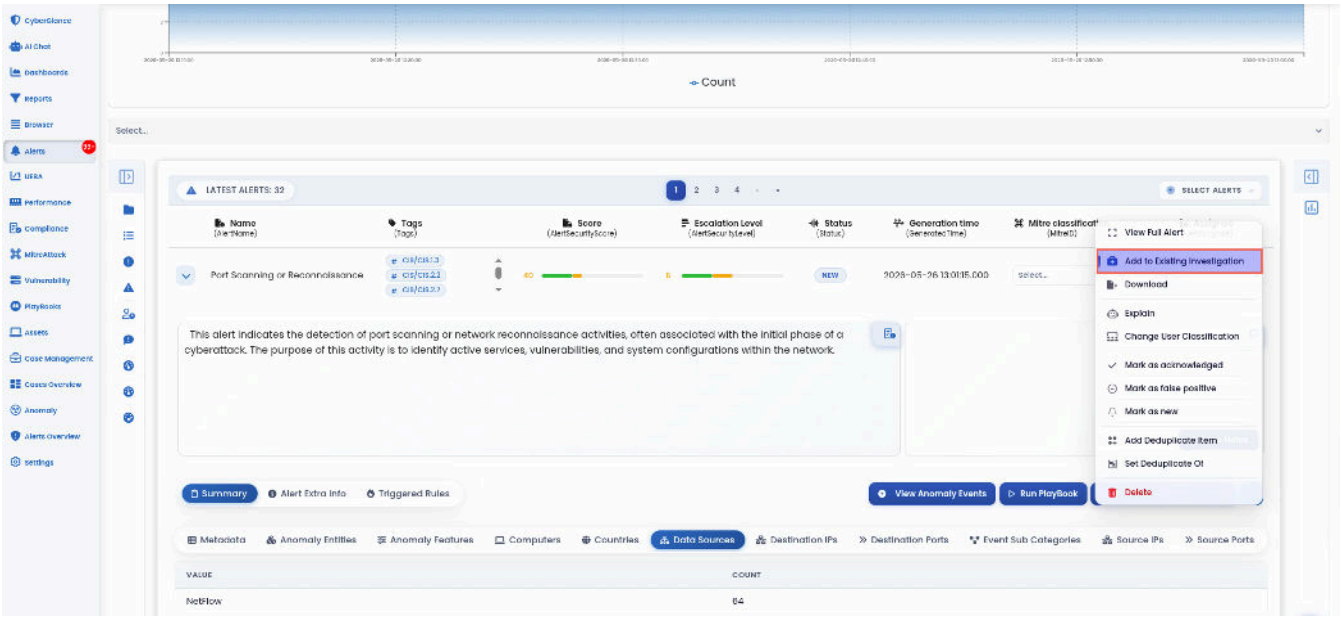
To create or update a case from an alert:

1. Navigate to the **Alerts** module and locate the alert that requires investigation.
2. Click the

   button to expand the alert details.

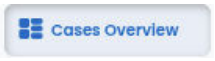
3. From the expanded alert view, use one of the available investigation actions:
   - **Create Investigation Case** - Opens a new case creation window and automatically adds the selected alert as evidence for the new case.
   - **Add to Existing Investigation** - Adds the selected alert as evidence to an already existing case. This option is available from the alert actions menu by clicking the **three-dot menu** on the right side of the alert action bar.





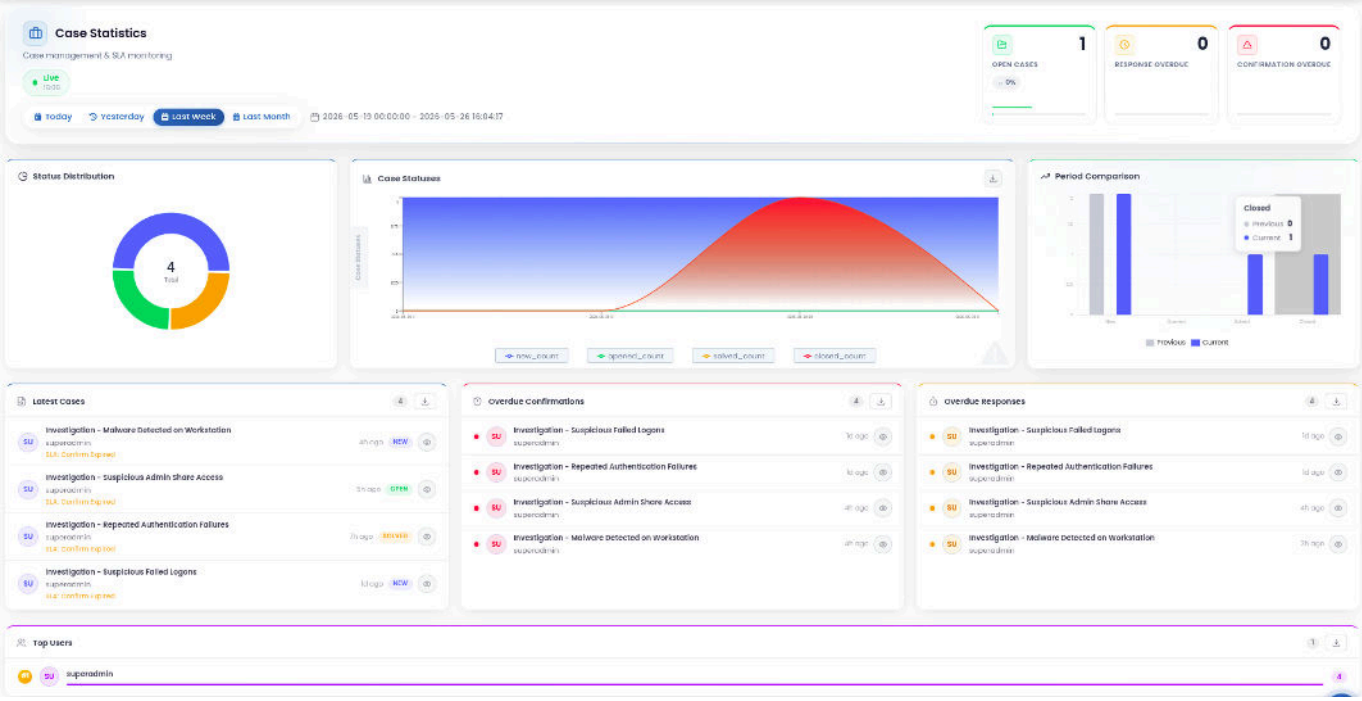
Case Overview

The **Case Overview** module provides a graphical summary of case activity across the organization. It can be accessed at any time by clicking the



button from the quick access menu on the left side of the web interface.

This view helps users monitor case volume, investigation progress, overdue confirmations, overdue responses, user workload, and status distribution within a selected time range.



The top section displays the main case indicators:

1. **Open Cases** - Shows the total number of cases currently marked with the **Open** status.
2. **Response Overdue** - Shows the number of cases where the configured response time has been exceeded.
3. **Confirmation Overdue** - Shows the number of cases where the configured confirmation time has been exceeded..

The date range selector allows users to filter the displayed information by predefined intervals such as **Today**, **Yesterday**, **Last Week**, or **Last Month**. The selected interval controls the data shown in the charts and summary panels.

The dashboard includes the following sections:

4. **Status Distribution** - Displays the distribution of cases by status, such as **New**, **Open**, **Solved**, **Closed**, and **Archived**.
5. **Case Statuses** - Shows how case statuses evolved over the selected time interval.
6. **Period Comparison** - Compares case status values between the current and previous selected periods.
7. **Latest Cases** - Displays the most recently modified cases, including case name, owner, status, and confirmation/response state.
8. **Overdue Confirmations** - Lists cases where the confirmation time has been exceeded.
9. **Overdue Responses** - Lists cases where the response time has been exceeded.
0. **Top Users** - Displays the users associated with the highest number of cases, helping identify workload distribution across analysts or teams.

To export data from the **Case Overview** in CSV format, click the

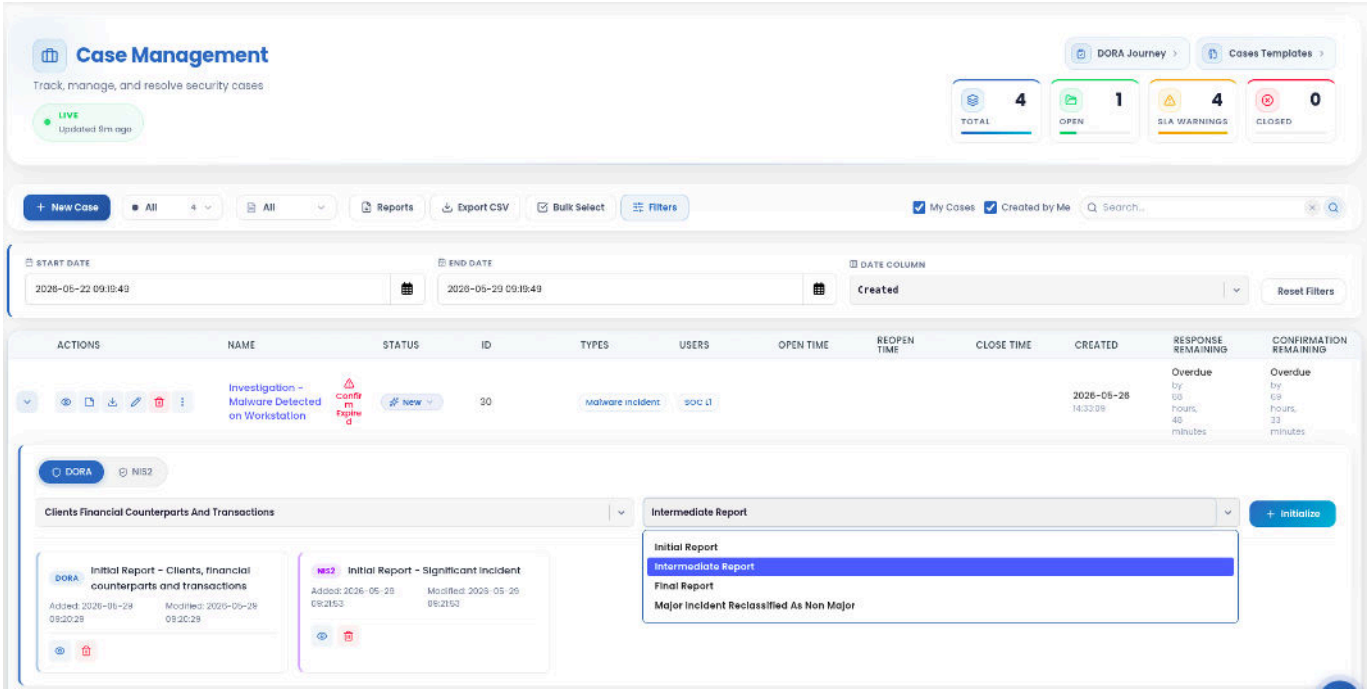


button.

CYBERQUEST - DORA Regulatory Assistance Module

The **DORA Regulatory Assistance module** extends the **CYBERQUEST Case Management** workflow with dedicated support for incident handling and regulatory reporting under the **Digital Operational Resilience Act (DORA)**.

The module helps security teams document, classify, and report ICT-related incidents in a structured and traceable manner. It supports the creation of regulatory reports based on the reporting structure defined by DORA and the related EU implementing regulation: EUR-lex (https://eur-lex.europa.eu/eli/reg_impl/2025/302/oj/eng)



The DORA module enhances the Case Management environment with dedicated regulatory assistance features:

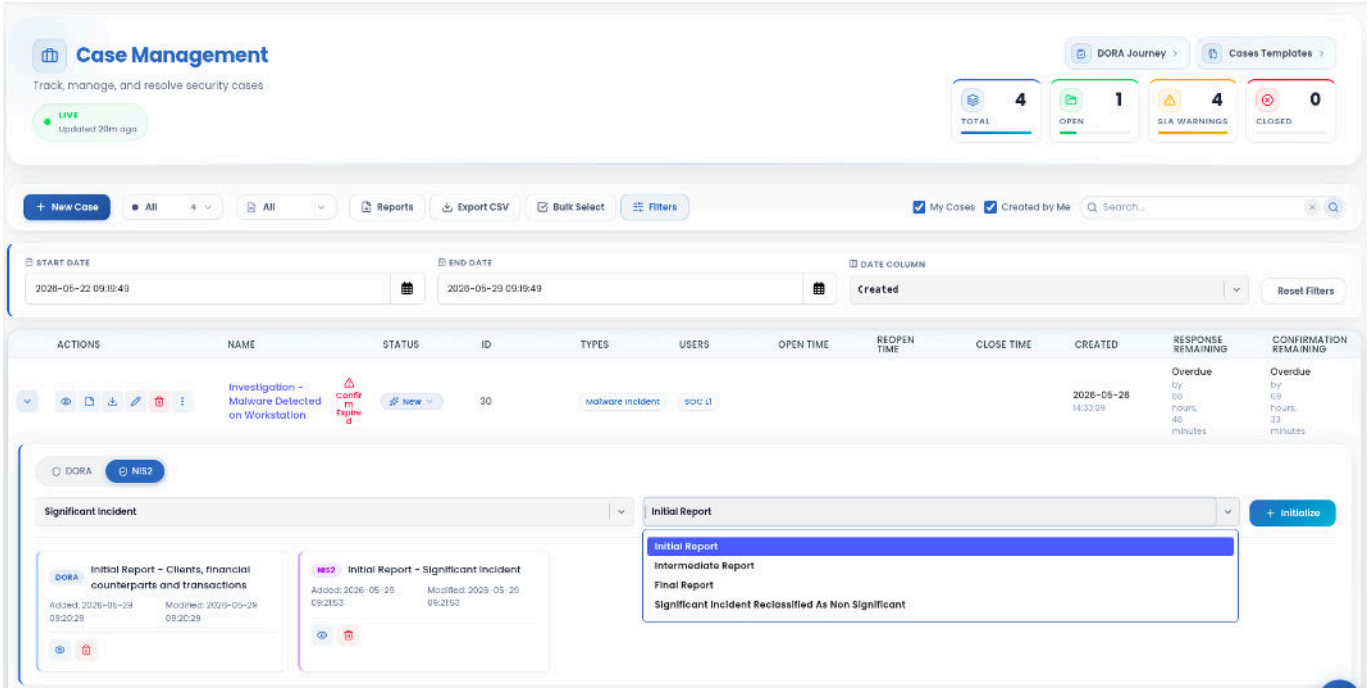
- **DORA Journey** - Provides a dedicated interface for following DORA-related compliance and readiness activities. It helps organizations track progress, identify gaps, and organize the steps required to support operational resilience and regulatory alignment.
- **Incident Reporting** - Allows users to generate structured incident reports directly from a case. Depending on the reporting stage, users can initialize report types such as **Initial Report**, **Intermediate Report**, **Final Report**, or **Major Incident Reclassified as Non-Major**.
- **Standardized Report Structure** - Helps ensure that incident reports follow a consistent format aligned with DORA reporting expectations. This reduces manual effort and supports more reliable documentation during incident response.
- **Case-Based Evidence Collection** - Links regulatory reporting with investigation data already available in the case, including alerts, evidence, notes, timelines, status changes, and assigned users.
- **Incident Classification Support** - Enables analysts to classify incidents according to the selected regulatory context, helping determine whether an event requires formal reporting or internal handling.

By integrating DORA reporting into the investigation workflow, CYBERQUEST helps organizations move from detection and case management to structured regulatory documentation, reducing reporting effort and improving audit readiness.

CYBERQUEST - NIS2 Regulatory Assistance Module

The **NIS2 Regulatory Assistance module** extends the **CYBERQUEST Case Management** workflow with dedicated support for incident documentation and reporting under the **NIS2 Directive**. NIS2 aims to establish a high common level of cybersecurity across the European Union and introduces cybersecurity risk-management and reporting requirements for essential and important entities.

The NIS2 module helps security teams manage significant incidents in a structured and traceable way, directly from an investigation case. Users can select the **NIS2** reporting option, choose the relevant incident category, and initialize the appropriate report type.



The available NIS2 report types include:

- **Initial Report** - Used to create the first incident report when a significant incident is identified and requires formal documentation.
- **Intermediate Report** - Used to provide updated information as the investigation progresses or when additional findings become available.
- **Final Report** - Used to document the completed investigation, including impact, root cause, actions taken, and final conclusions.
- **Significant Incident Reclassified as Non-Significant** - Used when an incident initially considered significant is later reassessed and no longer meets the reporting criteria.

The NIS2 module enhances the Case Management environment with dedicated regulatory assistance features:

- **Incident Reporting** - Allows users to generate structured reports directly from a case, keeping the investigation context linked to the reporting process.
- **Case-Based Evidence Collection** - Uses case information, evidence, notes, timelines, and related alerts to support incident documentation.
- **Standardized Report Structure** - Helps ensure that NIS2 incident reports follow a consistent format, reducing manual effort and supporting audit readiness.
- **Incident Classification Support** - Helps analysts classify and manage incidents according to the selected NIS2 reporting context.

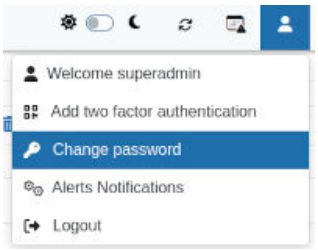
By integrating NIS2 reporting into the case workflow, CYBERQUEST helps organizations connect security operations with regulatory documentation, making incident handling more consistent, traceable, and easier to review.

User Actions

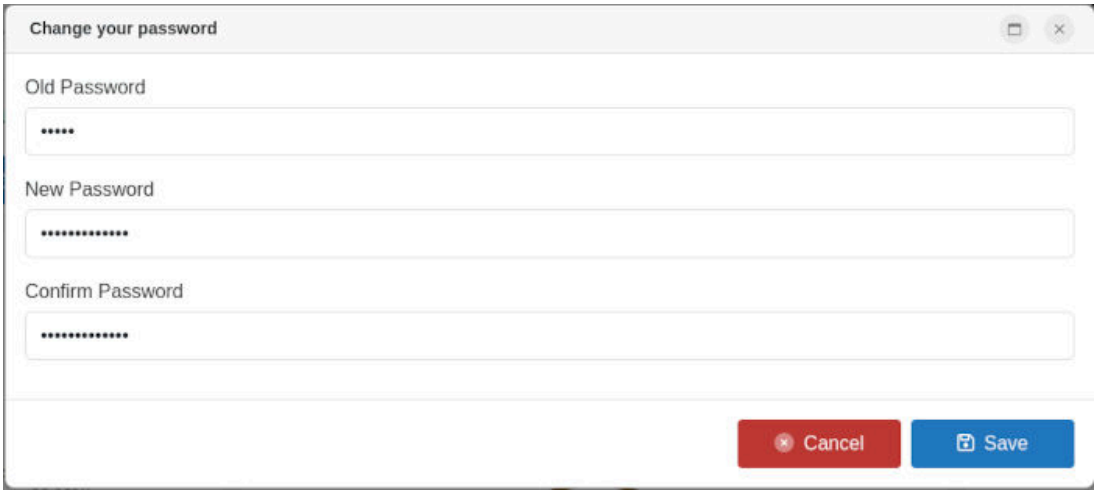
Changing Password

After successfully logging in, users can update their password at any time through the **User** menu. It is highly recommended to change the default password immediately after the first login to enhance account security.

To update the password, go to **Users > Change Password** from the navigation menu.



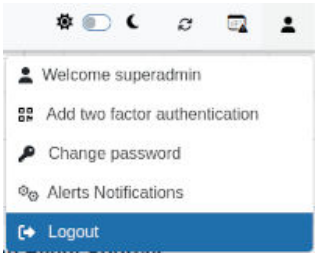
Once the **Change Password** window opens:



a. In the **Old Password** field, enter the current password. b. In the **New Password** field, enter the desired new password. Ensure it meets the complexity requirements defined by your organization. c. Re-enter the new password in the **Confirm Password** field. d. Click **Save** to apply the changes and close the window. To discard changes, click **Cancel**, or close the window using the

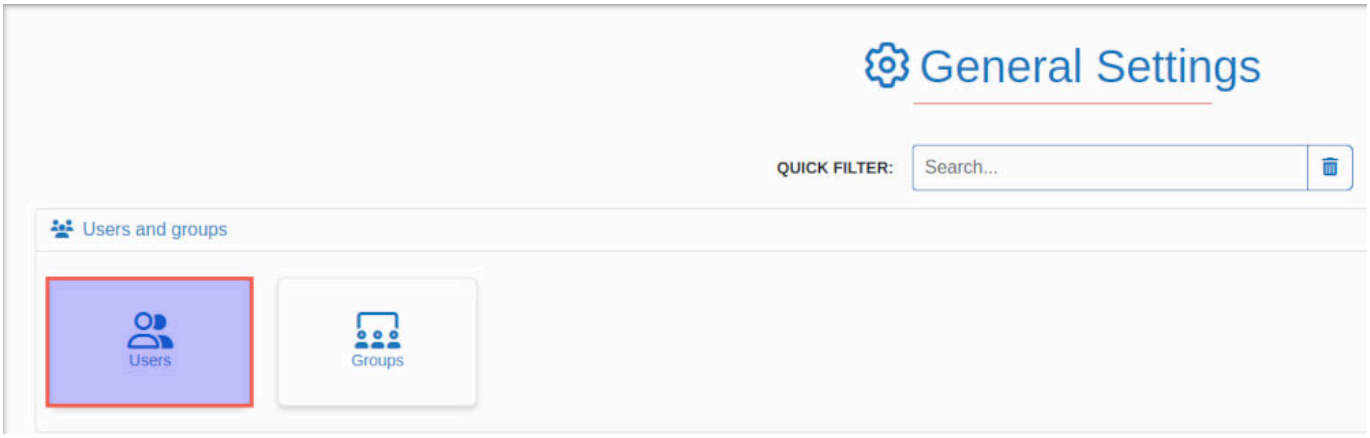
×

icon in the top-right corner. e. After changing the password, it is recommended to log out by selecting User > Logout from the User menu.

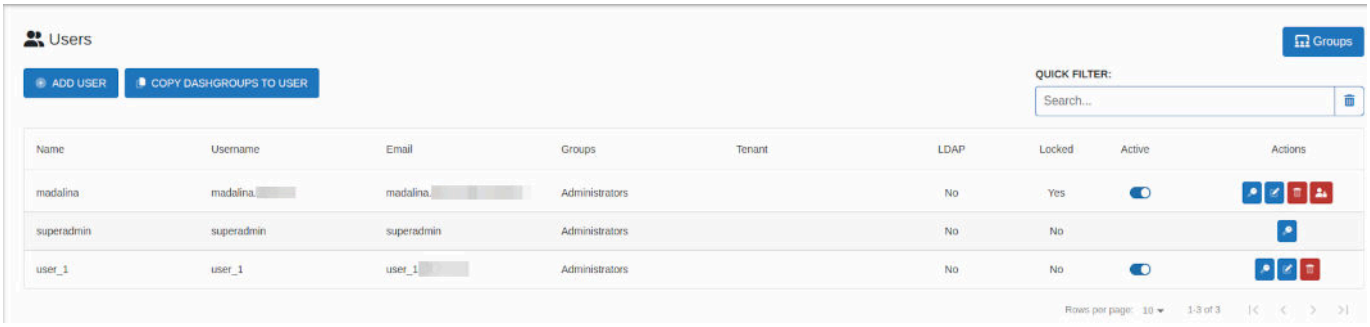


An administrator with user management rights can update their own password as well as reset passwords for other users. To perform this action:

a. From the **Settings** menu, navigate to **Users and Groups > Users**:



The **Users** configuration page will open:



b. Click the



button next to your name or the user whose password you want to update. This opens the **Change User Password** window:



c. Enter the new password in both the *New Password* and Confirm Password fields.

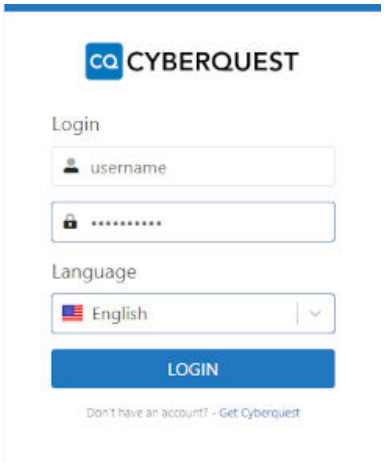
d. Click *Save* to apply the new password and close the window. To exit without saving, press *Cancel* or click the

mark in top-right corner.

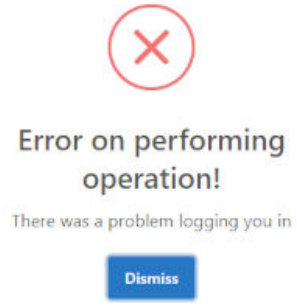
e. It is recommended to inform the user to log out and log back in using the new password to ensure the update takes effect.

Lock/unlock a user account

To access the CYBERQUEST Web Application, enter valid login credentials:

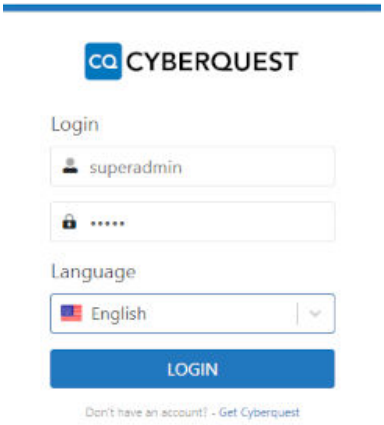


An account becomes **locked** after more than six consecutive failed login attempts. When this happens, an error message appears indicating that access is blocked:



To **unlock** the account, a **CYBERQUEST administrator** must perform the recovery process. The administrator needs to:

- Sign in to the CYBERQUEST Web Application using administrator credentials:

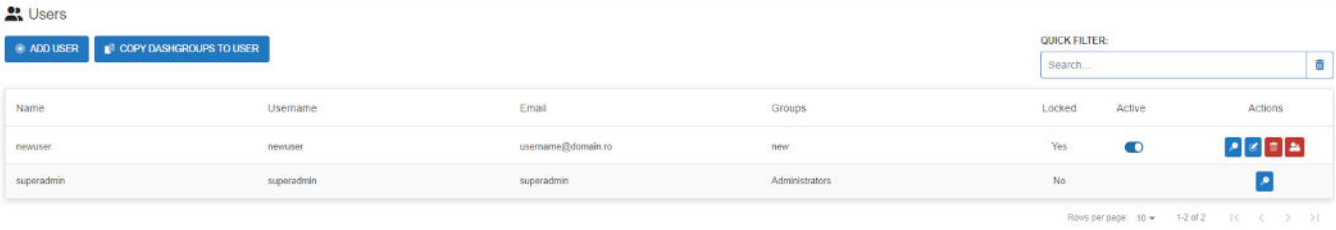


- Navigate to **Settings > Users and Groups > Users**.

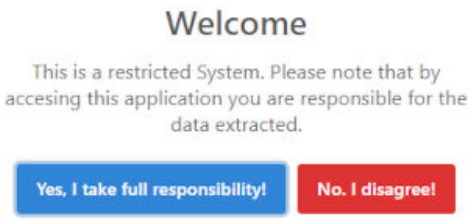
  Locate the locked user account, then click the

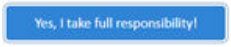
  button to unlock it:



- Once the account is unlocked, the user should attempt to log in using their credentials. A successful login will display the confirmation message:



  To proceed, select



to accept responsibility. Selecting



redirects to the authentication page.

Adding/removing 2FA

How to enable two-factor authentication (2FA) to an user account

Two-factor authentication (2FA) adds an additional layer of security by requiring both a password and a verification code generated by Google Authenticator. To activate 2FA, follow the steps outlined below:

Authentication

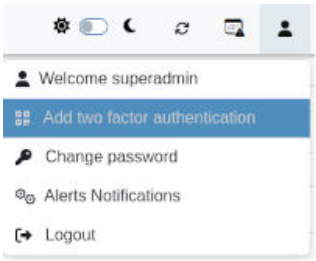
To access Web Interface, open a web browser and type the application's address or DNS name. The default address initially assigned to Web Interface is: ***https://CyberquestIPAddress*** (example).

The browser automatically redirects you to CYBERQUEST's authentication page:



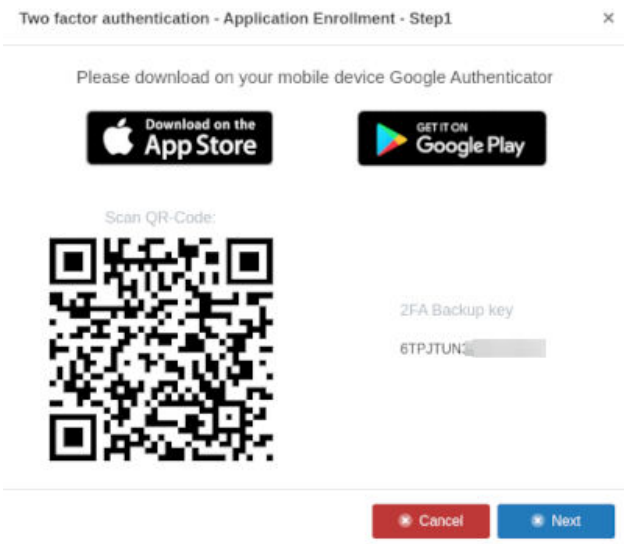
Navigate to Settings

Go to the **Settings** menu and select **Add Two-Factor Authentication**. This action will open the **Add Two-Factor Authentication** page:



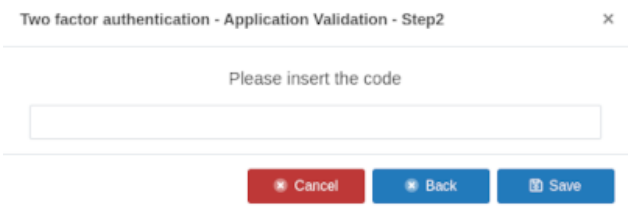
Application Enrollment

Use the Google Authenticator app to either scan the QR code or manually enter the 2FA backup key. Once completed, click the **"Next"** button to proceed.



Application Validation

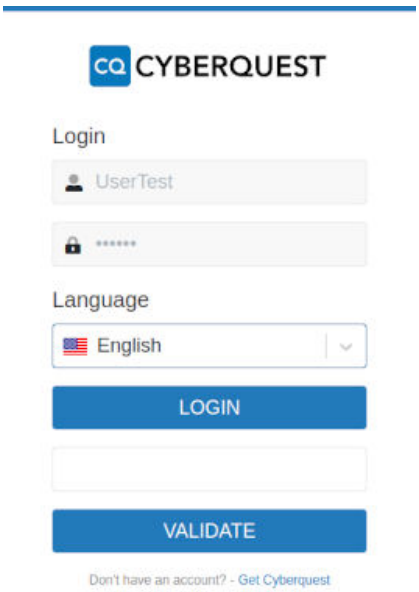
Enter the verification code generated by Google Authenticator, then click the **"Save"** button to complete the setup.



Login using 2FA

A. Sign in to the CYBERQUEST application using the assigned username and password.

B. Enter the verification code from the Google Authenticator app, then click the **"Validate"** button to proceed.



How to disable two-factor authentication (2FA) to an user account

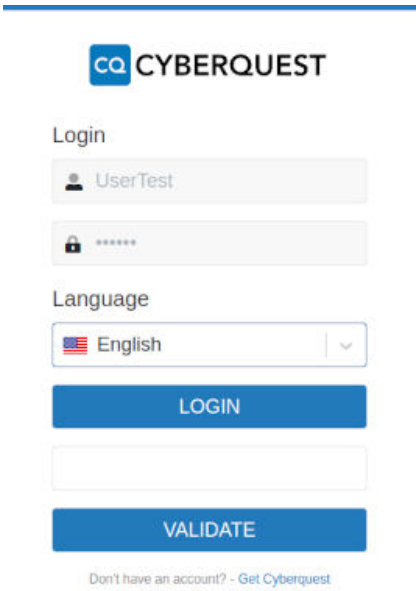
Two-factor authentication can be disabled in two ways:

- Disable your 2FA as User
- Disable 2FA as Administrator

1.Disable your 2FA as User

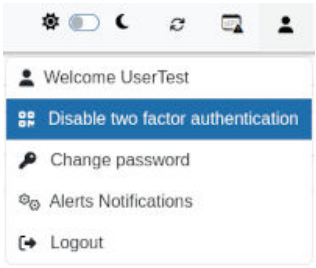
Login using 2FA

A. Sign in to the CYBERQUEST web application using the assigned username and password. B. Enter the verification code from the Google Authenticator app and click the **"Validate"** button.



Disable 2FA authentication

Navigate to the **Settings** menu and select **Disable two-factor authentication**. Once two-factor authentication is disabled, the session will be ended and the user will be logged out of the CYBERQUEST application.



2.Disable 2FA as Administrator

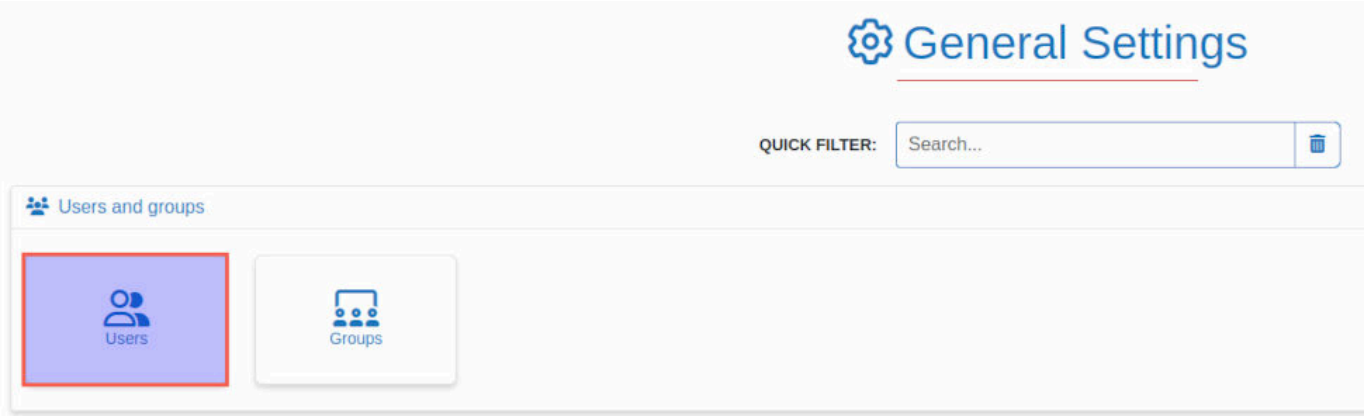
Authentication

Log in to the CYBERQUEST web application using an Administrator account. Open a web browser and enter the application's address or DNS name. By default, the Web Interface is initially accessible at: ***https://CyberquestIPAddress*** (example).



Navigate to Settings

Navigate to the **Settings** menu and select **Users and groups > Users**. This will open the **Users** page.

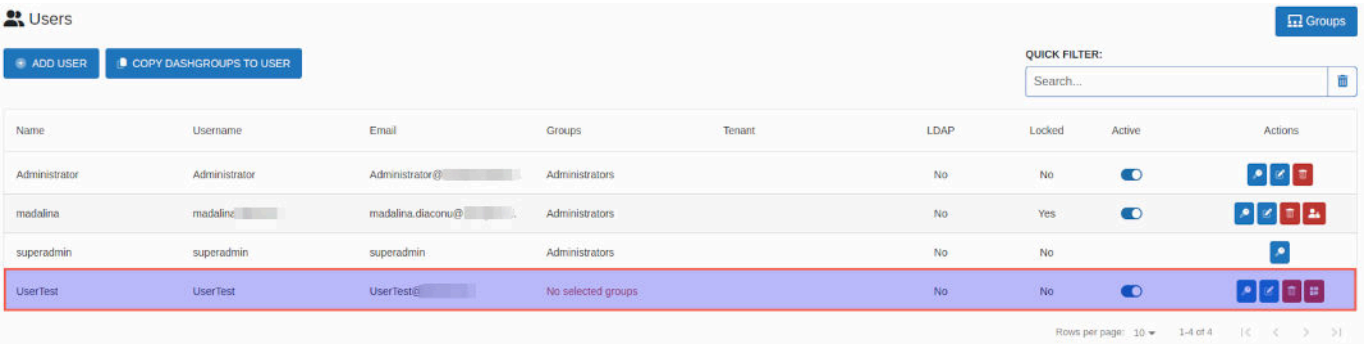


Disable 2FA authentication

On the **Users** page, choose the user for whom 2FA should be disabled and click the



bbutton to deactivate 2FA.



Threat Intelligence

Overview

Overview

What is Threat Intelligence?

Threat Intelligence is structured information about known or suspected cyber threats, such as malicious IP addresses, suspicious domains, TOR exit nodes, and other indicators of compromise. In CYBERQUEST, this information is used to enrich detection, improve event analysis, and support faster identification of potentially malicious activity.

Threat intelligence helps security teams answer key investigation questions:

- **What** indicators are associated with known threats?
- **Where** is suspicious activity coming from?
- **Which** IP addresses or domains should be monitored or blocked?
- **How** can threat context improve alert analysis and response?

The Value of Threat Intelligence

Threat intelligence helps transform raw security data into actionable context. Instead of analyzing events without background information, analysts can compare network activity, logs, and alerts against known malicious indicators.

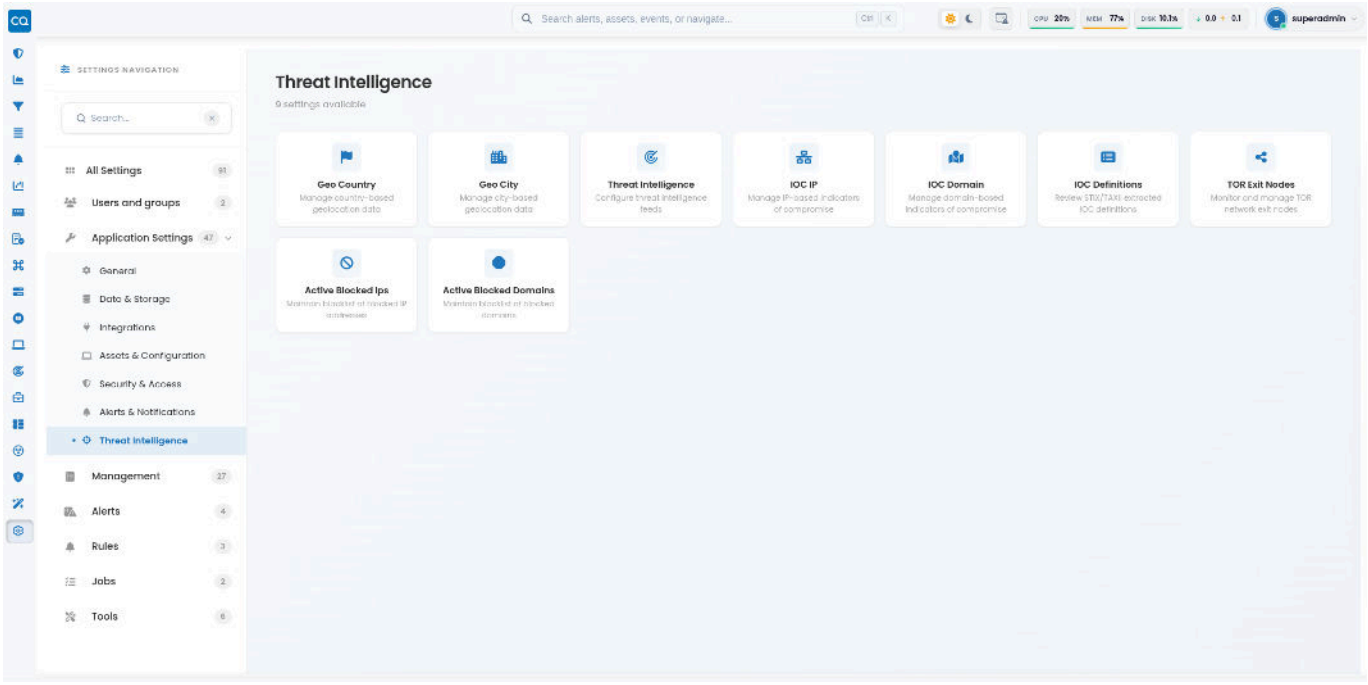
Key benefits include:

- **Proactive defense:** Enabling organizations to anticipate and prepare for threats before they materialize, rather than simply reacting to incidents after they occur.
- **Risk prioritization:** Helping security teams focus their efforts on the most relevant and high-impact threats to their specific environment.
- **Faster incident response:** Providing contextual information that accelerates investigation and response times during security incidents.
- **Strategic decision making:** Supporting executive-level decisions about security investments, risk management, and resource allocation.

Threat Intelligence Settings in CYBERQUEST

The **Threat Intelligence** settings section allows administrators to configure and manage threat intelligence sources used by CYBERQUEST. These sources can include IP-based feeds, domain indicators, TOR exit nodes, and active blocklists.

To access this section, go to **Settings > Application Settings > Threat Intelligence**.



The Threat Intelligence settings area displays the available configuration categories, including:

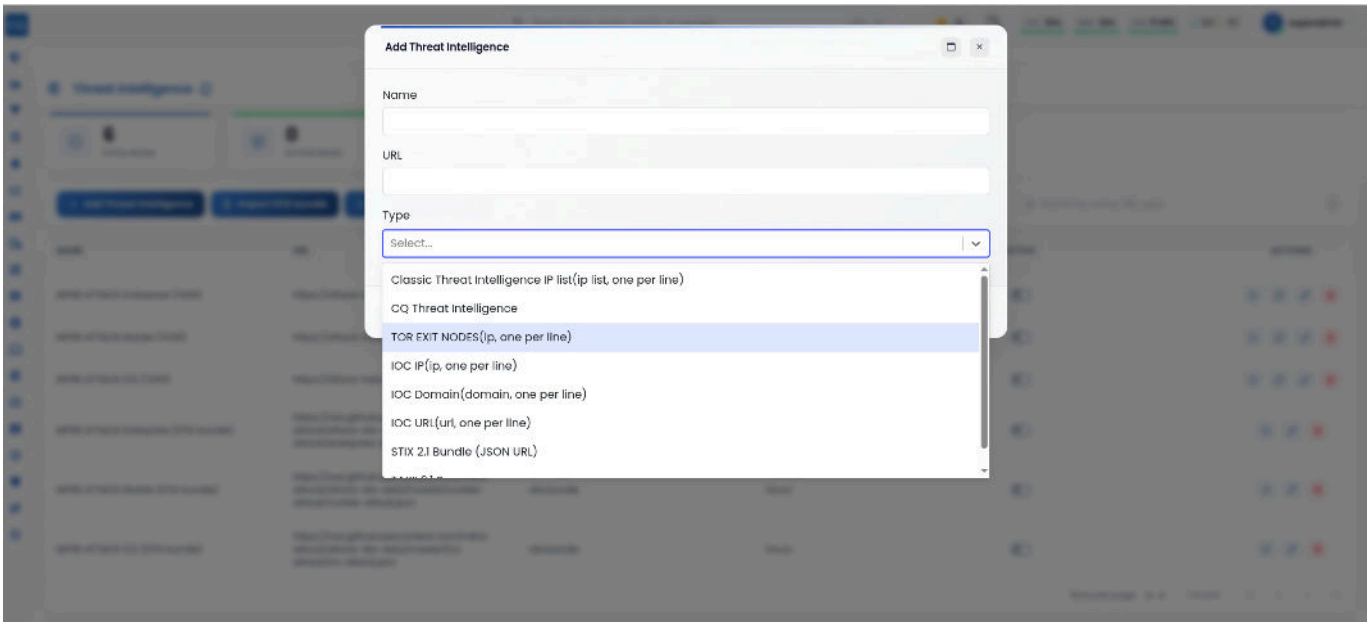
- **Geo Country** - Manages country-based geolocation data.
- **Geo City** - Manages city-based geolocation data.
- **Threat Intelligence** - Configures threat intelligence feeds.
- **IOC IP** - Manages IP-based indicators of compromise.
- **IOC Domain** - Manages domain-based indicators of compromise.
- **TOR Exit Nodes** - Monitors and manages TOR network exit nodes.
- **Active Blocked IPs** - Maintains the active blacklist of blocked IP addresses.
- **Active Blocked Domains** - Maintains the active blacklist of blocked domains.

Add a Threat Intelligence Source

To add a new threat intelligence source, click the



button. This opens the configuration window where a new source can be defined.



The following fields are available:

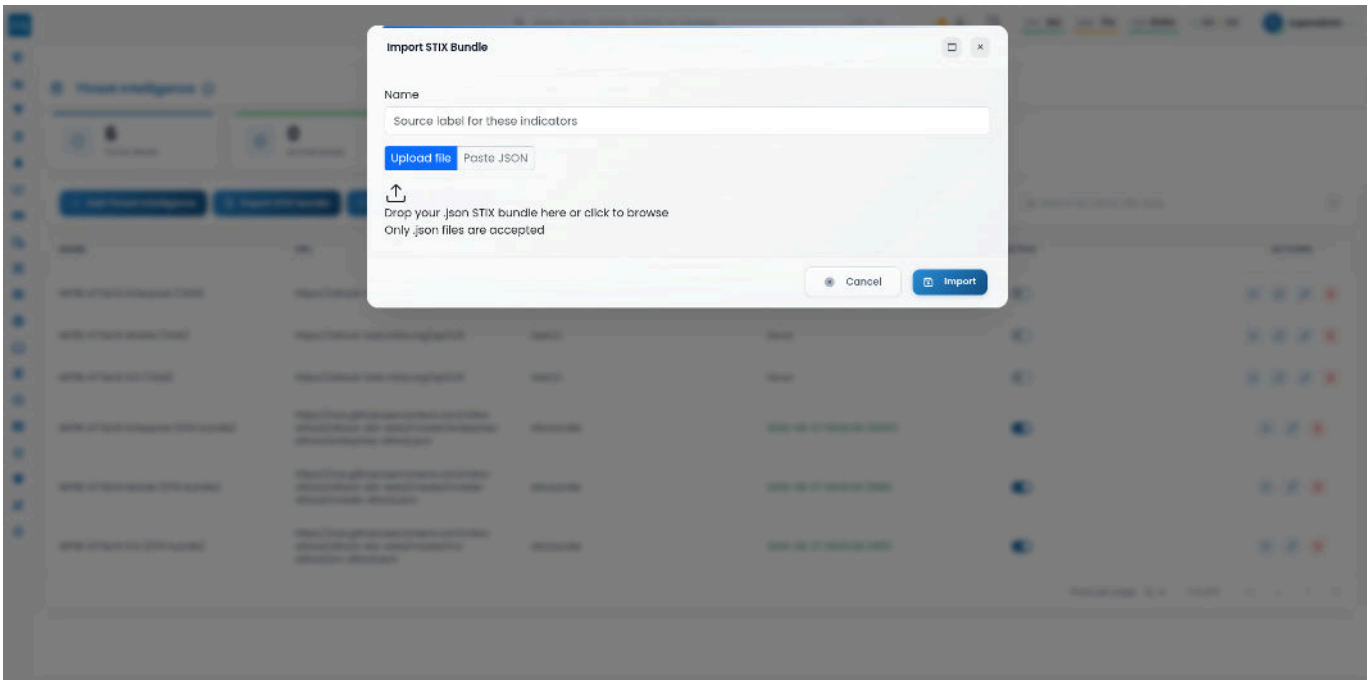
- **Name** - Defines the name of the threat intelligence source. Use a clear and descriptive name so the source can be easily identified later.
- **URL** - Specifies the location of the threat intelligence feed or source file. This can be used to retrieve the indicators that will be imported or processed by CYBERQUEST.
- **Type** - Defines the format and purpose of the threat intelligence source. The selected type determines how the imported data will be interpreted.

Available source types include:

- **Classic Threat Intelligence IP List** - Used for IP address lists, with one IP address per line. This is suitable for external or internal lists of suspicious or malicious IP addresses.
- **CQ Threat Intelligence** - Used for CYBERQUEST threat intelligence sources.
- **TOR Exit Nodes** - Used for lists of TOR exit node IP addresses, with one IP address per line. These indicators help identify traffic associated with TOR network exit points.
- **IOC IP** - Used for IP-based indicators of compromise, with one IP address per line. These indicators may represent malicious infrastructure, command-and-control servers, or attacker-controlled systems.
- **IOC Domain** - Used for domain-based indicators of compromise, with one domain per line. These indicators may include phishing domains, malware distribution domains, or suspicious command-and-control domains.
- **IOC URL** - Used for URL-based indicators of compromise, with one URL per line. These indicators may include malicious websites, phishing pages, malware distribution URLs, or command-and-control endpoints.
- **STIX 2.1 Bundle (JSON URL)** - Imports STIX 2.1 content from a JSON bundle available at a specified URL.
- **TAXII 2.1 Server** - Connects CYBERQUEST to a TAXII 2.1 server for retrieving structured threat intelligence.

Configured Threat Intelligence sources are displayed in the **Threat Intelligence** page together with their source type, synchronization status, activation state, and available management actions.

CYBERQUEST also provides an **Import STIX bundle** option for manually importing STIX 2.1 content. The bundle can be provided either by uploading a `.json` file or by pasting the JSON content directly into the interface.

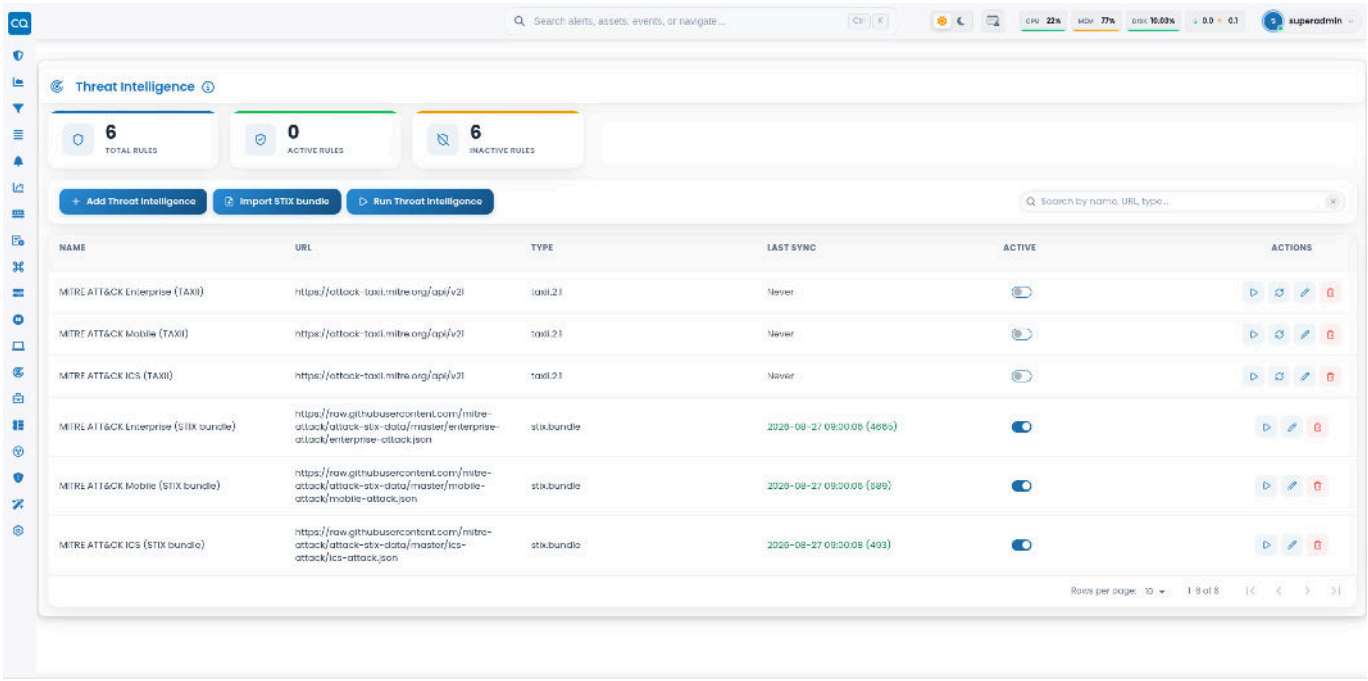


Imported STIX/TAXII content is processed by CYBERQUEST and made available through **IOC Definitions**, where the extracted definitions can be reviewed, searched, and inspected in detail: IOC Definitions

Managing Threat Intelligence Sources

After a threat intelligence source is created, administrators can manage it from the **Threat Intelligence** interface.

The interface displays the configured sources together with their **Name, URL, Type, Last Sync status, activation state, and available management actions**. The search field can be used to locate sources by name, URL, or type.



Available management actions may include:

- **Sync now**



  - Synchronizes the selected threat intelligence source and retrieves the latest available data.
- **Full re-sync (re-pull entire collection)**



  - Re-pulls the complete dataset from the selected threat intelligence source and performs a full synchronization.
- **Edit**



  - Updates the configuration of an existing threat intelligence source.
- **Delete**



  - Removes the selected threat intelligence source from the system.
- **Activate/Deactivate**



  - Enables or disables the source without deleting it.

The **Run Threat Intelligence**



button at the top of the page can be used to manually start the threat intelligence processing workflow for the configured sources.

The **Last Sync Information** column shows when a source was last synchronized and, where available, the number of definitions retrieved during that synchronization.

These options allow administrators to maintain threat intelligence sources, synchronize and refresh threat data, disable unused feeds, and ensure that relevant threat intelligence remains available for detection, enrichment, and investigation workflows.

Providers

Threat Intelligence Providers

CYBERQUEST integrates with multiple threat intelligence providers to deliver comprehensive cyber threat coverage. These partnerships enable organizations to leverage curated threat data from specialized security vendors, enhancing their ability to detect and respond to emerging threats.

Nucleon

Nucleon's cyber threat intelligence feeds provide organizations of all sizes with trusted, actionable cyber intelligence to proactively block or mitigate future attacks. These feeds are particularly valuable for organizations that may not have dedicated threat intelligence teams, as they can leverage intelligence gathered by Nucleon's specialized researchers to enhance their own security posture.

For more information, please access the link (https://nucleoncyber.com/cyber-intelligence/).

Dekeneas

DEKENEAS represents a significant advancement in web-based threat detection, utilizing artificial intelligence algorithms to identify both known and unknown browser exploits ("0day") with exceptional accuracy. Unlike traditional security solutions that rely on signature-based detection methods, DEKENEAS employs advanced AI techniques to analyze website code before execution, determining whether encountered code constructs are malicious or benign.

For more information, please access the link (https://www.dekeneas.com/products/).

CQ ThreatIntelligence

CYBERQUEST's proprietary threat intelligence feed combines external threat data with contextual information gathered from your organization's IT infrastructure, providing highly relevant and actionable intelligence. This unique approach ensures that threat intelligence is not only comprehensive but also specifically tailored to your environment.

How CQ ThreatIntelligence Works

CYBERQUEST's powerful correlation engine processes threat data in real-time by:

1. **Data collection**: Gathering threat intelligence from multiple high-value security providers and CYBERQUEST's own deployed sensors
2. **Contextual analysis**: Cross-referencing external threat data with information collected from the monitored IT infrastructur
3. **Real-time matching**: Continuously compares incoming data against a dynamic database of known threat indicators and behavioral patterns.
4. **Actionable intelligence:** Delivering prioritized alerts based on the relevance of threats to the specific operational environment

CQ ThreatIntelligence provides comprehensive coverage of key threat indicators, including:

- **Malicious IPs:** Addresses associated with known attack sources, botnet command and control servers, and other malicious infrastructure
- **Malicious Domains:** Websites identified as hosting malware, conducting phishing campaigns, or serving as command and control centers
- **Malicious URLs:** Specific web addresses linked to malicious activities, including exploit kits, malware downloads, and social engineering attacks

Access to CQ ThreatIntelligence requires a separate subscription, ensuring that customers receive the highest quality threat intelligence with regular updates and comprehensive coverage.

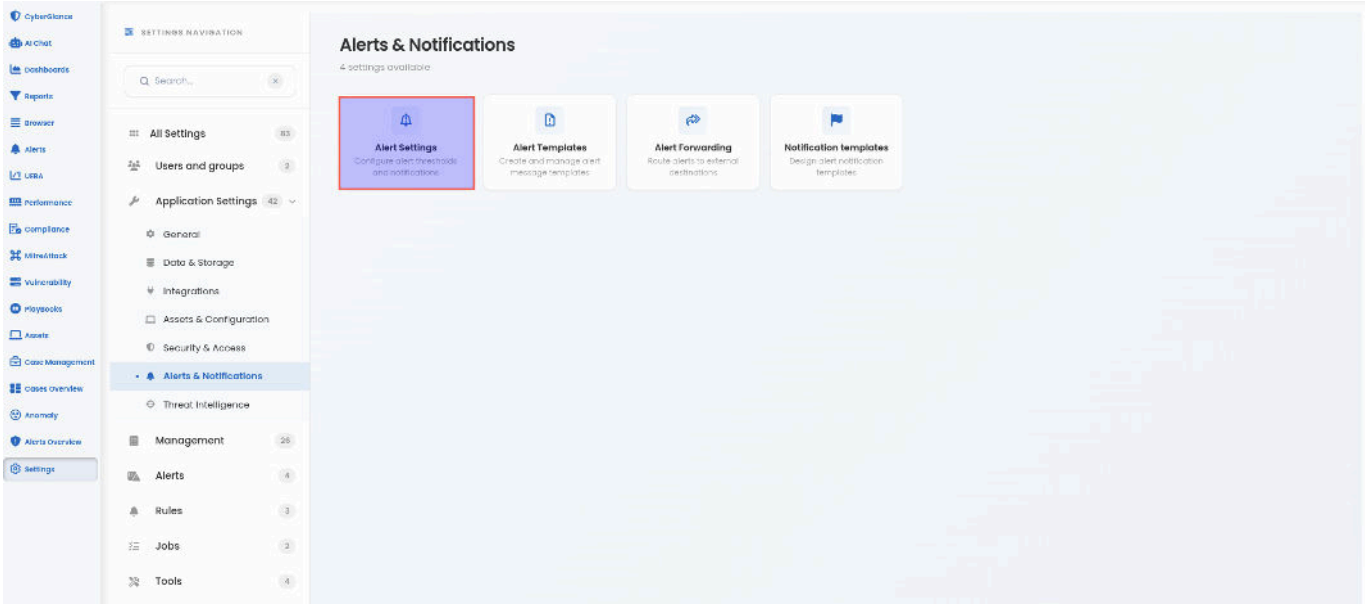
For detailed instructions on connecting to CQ Threat Intelligence, please follow the link: CQ Threat Intelligence

Built in Automatic Alerts

CYBERQUEST includes built-in automatic alerts that continuously monitor events and trigger notifications when specific security conditions are detected. These alerts use configured threat intelligence sources and predefined detection logic to identify suspicious activity, such as communication with blacklisted IP addresses or activity performed by blacklisted users.

Accessing Alert Settings

To configure and manage built-in automatic alerts, go to **Settings > Application Settings > Alerts & Notifications > Alert Settings**.



The **Alert Settings** page displays the available automatic alert settings. From this interface, administrators can search for alert settings, review their status, and enable or disable each alert depending on the organization's monitoring requirements.



The top section provides a quick summary of the alert settings:

- **Total Settings** - Displays the total number of available alert settings.
- **Enabled** - Displays how many alert settings are currently active.
- **Filtered** - Displays how many settings match the current filter or search criteria.

Each alert setting includes an **Active** toggle that allows administrators to enable or disable the alert without removing the configuration.

Available Built-in Alert Settings

Alerts_Blacklisted_IPs

The **Alerts_Blacklisted_IPs** setting monitors events against known blacklisted IP addresses from configured Threat Intelligence sources. When enabled, CYBERQUEST can detect activity involving IP addresses that are considered suspicious or malicious.

This alert supports two detection scenarios:

- **IP Match:** Triggers when an event contains an IP address that matches an entry from the blacklisted IP sources. This helps identify active communication with known malicious or suspicious infrastructure.
- **Backwards IPMatch:** Performs retrospective detection when new IP addresses are added to the blacklist. CYBERQUEST checks historical data to identify previous events that involved those IP addresses, helping analysts discover earlier activity that may not have been identified at the time.

Alerts_Blacklisted_Users

The **Alerts_Blacklisted_Users** setting monitors activity associated with user accounts that are included in a blacklist or threat intelligence source. When enabled, the alert triggers when events are detected for users that have been marked as suspicious, compromised, or requiring special monitoring.

This helps security teams detect activity from high-risk accounts and investigate possible unauthorized access, account compromise, or policy violations.

CQ TI IPMatch

CQ TI IP Match is a real-time detection mechanism that checks event IP addresses against the CYBERQUEST Threat Intelligence feed. If an event contains an IP address that matches a known malicious or suspicious indicator, CYBERQUEST can generate an alert for further investigation.

CQ TI Backwards IPMatch

CQ TI Backwards IP Match provides retrospective threat detection. When new malicious IP addresses are added to the threat intelligence database, CYBERQUEST can check historical events to determine whether those IPs were previously observed in the environment.

CQ TI Domain Match

Q TI Domain Match monitors events for domains identified as malicious or suspicious in the CYBERQUEST Threat Intelligence feed. When an event contains a domain that matches an indicator from the domain blacklist, CYBERQUEST can generate an alert.

Batch Fields Checker

The Batch Fields Checker is a powerful tool that allows security analysts to perform bulk validation of potential threat indicators against CYBERQUEST's data stores. This feature is particularly useful for analyzing large lists of suspected malicious entities without manually checking each one.

To use the Batch Fields Checker for uploading a text file and executing batch checking of selected fields (like as a list of malicious IPs), please follow the link: Batch fields checker.

Correlation

Introduction of Correlation

Introduction to Correlation

A correlation rule serves as an intelligent template that defines specific conditions and relationships between different events, enabling the detection of complex threats that might not be apparent when examining individual logs in isolation.

This service allows the user to correlate events based on data correlation rules that accommodate different needs, like as: brute force attack prevention, abnormal user behaviour, virus attacks (and/or propagation), application misbehaviour, etc.

How Correlation rules work

Correlation rules are advanced logic-based rules used to analyze and link related security events within the system:

- **Combine Multiple Events:** Analyze data from diverse sources such as firewalls, intrusion detection systems, authentication logs, and application logs
- **Define Temporal Relationships:** Define timeframes in which related events must occur to trigger an alert
- **Establish Event Sequencing:** Specify the order in which events should happen to identify attack patterns
- **Apply Conditional Logic:** Apply specific conditions to differentiate between normal behavior and potential threats

For more detailed information about correlation and its implementation in CYBERQUEST, please refer to the following resources:

Alerts Module

Data flow rules and filters

How to create new alerts

How to create a DTS Alert

Types of Correlation

The system supports two primary correlation approaches for alert configuration:

- **Single Event Alert** - These alerts trigger based on individual events matching specific criteria.
  Example: Administrator logons detected outside business hours.

- **Correlated Events** - Multiple rules connected through shared fields, executed sequentially within a defined time window. This approach enables complex alert logic through event chains.

Alert/Action methods for Correlated events

- **Single Event Trigger:** Activates when the first matching event correlates with previous events in the chain.
- **Multiple Events Trigger:** Requires configurable conditions:
  - **Rule Trigger Type:** Single Event Trigger, Count-based, Sum-based, Average-based, Distinct Count-based
  - **Min. Threshold:** Minimum value to trigger after time window expires
  - **Max. Threshold:** Maximum value to trigger before time window expires
  - **TTL (Time to Live):** Duration in seconds for correlation window
  - **Pivot Field:** Numeric field used for threshold calculations

Rule Trigger Types

- **Count-Based Trigger:** Activated when the number of matching events reaches the maximum threshold before the TTL (Time to Live) expires, or when the minimum threshold is met upon TTL expiration.
- **Sum-Based Trigger:** Activated when the sum of a numeric field (defined in the Pivot Field setting) is greater than or equal to the maximum threshold before TTL expires, or greater than or equal to the minimum threshold at TTL expiration.
- **Average-Based Trigger:** Activated when the average of a numeric field (defined in the Pivot Field setting) is greater than or equal to the minimum threshold at TTL expiration.
- **Distinct Count-Based Trigger:** Distinct Count-Based Trigger: Activated when the number of unique values from a specified field reaches the maximum threshold before the TTL (Time to Live) expires, or when it reaches the minimum threshold upon TTL expiration.

Three condition types enable precise event matching:

- *FIELD CONDITION* - Compare event fields with static values.
- *REPORT CONDITIONS* - Allows comparison between the current event and a predefined report selected by the user.
- *CORRELATION CONDITION* - Enables comparison between a value in the current event and a value from previous events within the correlation chain.

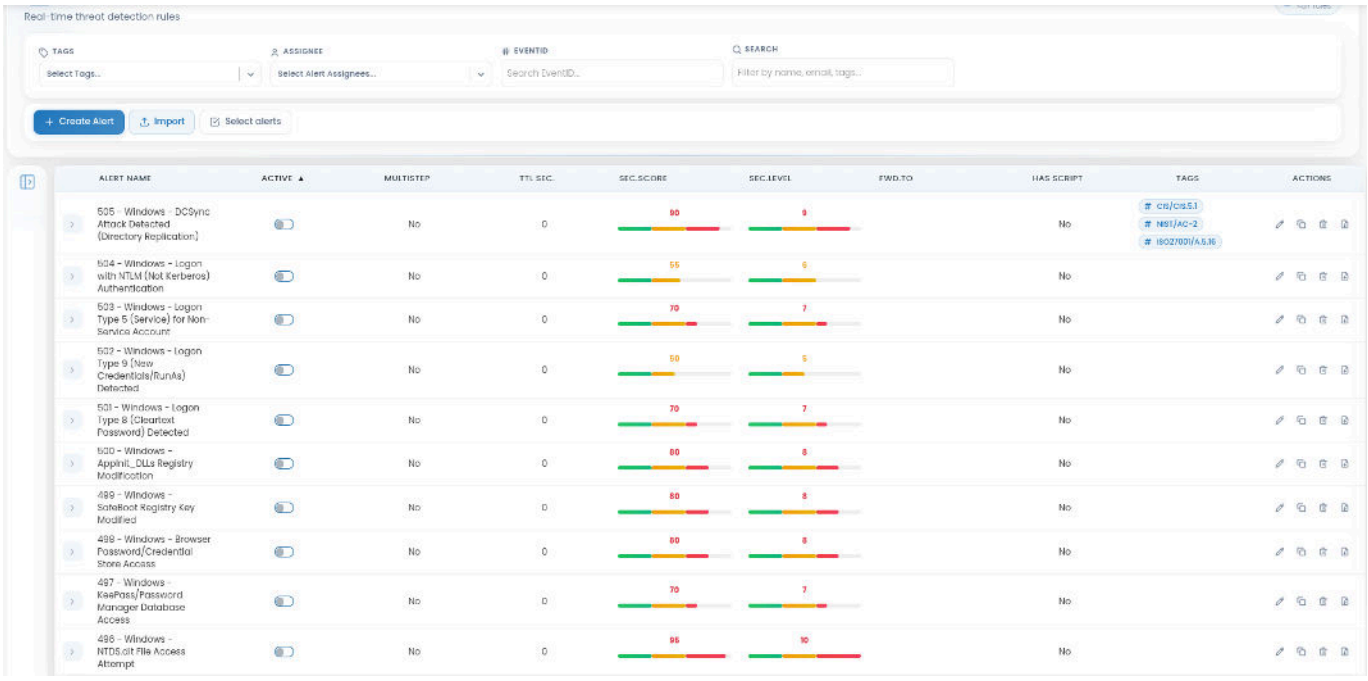
For additional information on alerts, refer to the following link: Alerts Module

Data Transformation Service (DTS) Module - Using advanced filters, events can be matched to a Data Acquisition Rule (DA Rule), which applies a transformation script to allow further customization. This enables direct interaction with the event data and the ability to define long-term storage options. Additionally, the module supports actions such as sending alerts or emails, temporarily storing or retrieving data for future correlation, querying historical events in short-term storage (Online DataStorage), or dropping events as needed.

For additional information on DTS, refer to the following link: How to create a DTS Alert

Managing Correlation Alerts

To manage correlation alerts, navigate to **Settings > Alerts > Realtime**. This page displays the realtime correlation rules available in CYBERQUEST and allows administrators to review, enable, disable, import, export, clone, or edit alert definitions.



The **Realtime** page includes filtering options that help users quickly locate specific alert rules:

- **Tags** - Filters alerts based on assigned tags.
- **Assignee** - Filters alerts by the assigned alert owner or responsible user.
- **EventID** - Searches alerts by the configured event identifier.
- **Search** - Allows searching for alerts by **alert name**.

The alert table displays key configuration details for each rule, including alert name, active status, multistep configuration, TTL, security score, security level, forwarding destination, script usage, tags, and available actions. Manage alerts using the available interface actions:

- **Create a new alert**: Click

  to open the **Alert Settings** window and define a new custom alert. For detailed instructions, refer to the Create New Alert.
- **Import**: Click

  to import an alert definition from an existing CQO file.
- **Select Alerts**: Enables selection of multiple alerts for bulk operations.
- **Alert details**

  : Expands or opens detailed information about the selected alert, including its configuration and triggering conditions.
- **Enable/Disable alert**:Use the active switch to control whether the alert is enabled or disabled. The

  icon indicates an active alert, while the

  icon indicates an inactive alert.
- **Edit alert**

  : Opens the alert configuration so the rule definition can be modified.
- **Clone alert**

  : Creates a copy of the selected alert, allowing users to reuse an existing configuration as a starting point for a new rule.
- **Delete alert**

  : Removes the selected alert definition from the system
- **Export alert**

  : Exports the selected alert definition as a CQO file, which can be used for backup, migration, or reuse in another environment.
- **Rows per page dropdown**: Allows users to choose how many alert rules are displayed in the table.

To view all triggered alerts, navigate to the **Alerts Module**. For comprehensive details about alert results, see the Alerts Results Section.

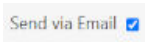
Default Correlation Alerts

Navigate to "***Settings > Alerts > Realtime***". In the **Realtime** page we will find all alerts defined in CYBERQUEST. These is a list with all default alers defined in CYBERQUEST:

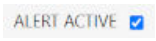
1. ***A computer account was removed from domain***

Description - A new event is generated containing details of *a computer account that was deleted from domain*. In Active Directory, when a computer is deleted, the **EventID** gets logged.

In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the condition. To receive the alert information via email, click the following options:



and set



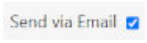
.

Prerequisites - Windows Security Log.

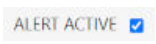
2. ***A computer account was added to domain***

Description - A new event is generated containing details of *a computer account that was created to domain*. In Active Directory, when a computer object is created, the **EventID** gets logged.

In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the condition. To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows Security Log.

3. ***UBA - User set to Non-Expiring Password***

Description - A new event is generated containing details of *a user that is set Enabled to Non-Expiring Password*. In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the conditions. To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows Security Log.

4. UBA - Restricted Domain Account Failed Logon

Description - A new event is generated when a logon request fails on the computer where access was attempted. The alert is generated when the event is registered with an status and sub-status code and is providing the information: "User logon from an unauthorized workstation".

In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the conditions. To receive the alert information via email, click the following options:



and set



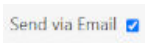
.

Prerequisites - Windows Security Log.

5. UBA - Failed Domain Logon on Restricted Host

Description - A new event is generated when a logon request fails. The alert is generated when the event is registered with an status and sub-status code and is providing the information: "User logon from an unauthorized workstation".

In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the conditions. To receive the alert information via email, click the following options:



and set



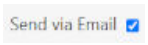
.

Prerequisites - Windows Security Log.

6. *UBA - Domain User Logon After Multiple Failed Attempts*

Description - A new event is generated containing details of *Domain User Logon After Multiple Failed Attempts*. In CYBERQUEST, this alert with 3 Rules will trigger on first event that will match the conditions: failed logon, Multiple Login Fails Count and 1 success.

To receive the alert information via email, click the following options:



and set



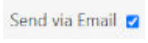
.

Prerequisites - Windows Security Log.

7. *UBA - Domain User Failed Logon Due to Invalid Password*

Description - A new event is generated containing details of *Domain User Failed Logon Due to Invalid Password*. The alert is generated when the event is registered with an status and sub-status code and is providing the information: "User logon with misspelled or bad password".

In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the condition. To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows Security Log.

8. ***UBA - User Logon from Multiple IP Addresses***

Description - A new event is generated when a logon session from multiple IP addresses is created. It generates on the computer that was accessed, where the session was created.

In CYBERQUEST, this alert with 2 Rules will trigger on first event that will match the conditions. To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows Security Log.

9. ***UBA - User Logon from Multiple Hosts***

Description* - A new event is generated containing details of *User Logon from Multiple Hosts*. Detects when a single user logs in from more than an allowed number of devices.

In CYBERQUEST, this alert with 2 Rules will trigger on first event that will match the conditions. To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows Security Log.

10. ***UBA - Username ending with Dollar Sign***

Description - A new event is generated containing details of *Username ending with Dollar Sign*. In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the condition. To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows Security Log.

11. ***UBA - Remote Login to Server***

Description - A new event is generated containing details of *UBA - Remote Login to Server*. In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the condition. To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows Security Log.

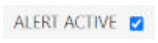
12. ***UBA - New User Observed***

Description - A new event is generated containing details of *New User Observed*. Detects when an account successfully used for the first time.

In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the condition. To receive the alert information via email, click the following options:



and set



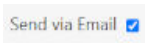
.

Prerequisites - Windows Security Log.

13. ***UBA - Login Attempt from User with Expired Password***

Description - A new event is generated containing details of *Login Attempt from User with Expired Password*. This alert detects when a user attempted to log in to a disabled or and expired account. The alert is generated when the event is registered with an status and sub-status code and is providing the information: "User logon with expired password".

In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the condition. To receive the alert information via email, click the following options:



and set



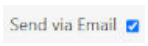
.

Prerequisites - Windows Security Log.

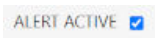
14. ***UBA - Login Attempt from Locked or Disabled Account***

Description - A new event is generated containing details of *Login Attempt from Locked or Disabled Account*. This alert detects when a user is trying to access the organization resources by using a disabled or locked account. The alert is generated when the event is registered with an status and sub-status code and is providing the information: "User logon from an unauthorized workstation".

In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the condition. To receive the alert information via email, click the following options:



and set



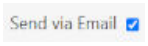
.

Prerequisites - Windows Security Log.

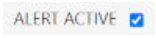
15. ***Domain Policy - User Removed from Local Security Group***

Description - A new event is generated every time member was removed from security-enabled local group.

In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the condition. To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows Security Log.

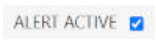
16. Domain Policy - User Removed from Domain Security Group

Description - A new event is generated every time member was removed from security-enabled domain group.

In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the condition. To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows Security Log.

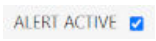
17. Domain Policy - User Added to Local Security Group

Description - A new event is generated every time member was added to a security-enabled local group.

In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the condition. To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows Security Log.

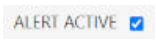
18. Domain Policy - User Added to Domain Security Group

Description - A new event is generated every time member was added to a security-enabled domain group.

In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the condition. To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows Security Log.

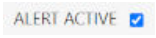
19. Domain Policy - Group Policy Object Modified

Description - A new event is generated containing details of *Group Policy Object Modified*. This event generates every time an Active Directory object is modified.

In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the condition. To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows Security Log.

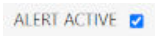
20. Domain Policy - Group Policy Object Created

Description - A new event is generated containing details of *Group Policy Object Created*. This event generates every time an Active Directory object is created.

In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the condition. To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows Security Log.

21. Domain Policy - Group Policy Object Deleted

Description - A new event is generated containing details of *Group Policy Object Deleted*. This event generates every time an Active Directory object is deleted.

In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the condition. To receive the alert information via email, click the following options:



and set



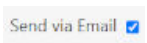
.

Prerequisites - Windows Security Log.

22. Domain Policy - Domain Policy Changed

Description - A new event is generated containing details of *Domain Policy Changed*. This event generates every time an Active Directory object is changed.

In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the condition. To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows Security Log.

23. Windows - Multiple Failed Packaged App Applocker Events - Multiple Hosts

Description - A new event is generated containing details of *Multiple Failed Packaged App Applocker Events - Multiple Hosts*. The alert generates if the message information: “Packaged app disabled” or “Packaged app installation audited”.

AppLocker can help you improve the management of application control and the maintenance of application control policies.

In CYBERQUEST, this alert with 2 Rules will trigger on first event that will match the conditions. To receive the alert information via email, click the following options:



and set



.

Prerequisites - Microsoft-Windows-AppLocker/Packaged app-Deployment.

24. Windows - Multiple Failed Packaged App Applocker Events - Single Host

Description - A new event is generated containing details of *Multiple Failed Packaged App Applocker Events - Single Host.* The alert generates if the message information: "Packaged app disabled" or "Packaged app installation audited".

AppLocker can help you improve the management of application control and the maintenance of application control policies.

In CYBERQUEST, this alert with 2 Rules will trigger on first event that will match the conditions. To receive the alert information via email, click the following options:



and set



.

Prerequisites - Microsoft-Windows-AppLocker/Packaged app-Deployment / Microsoft-Windows-AppLocker/Packaged app-Execution.

25. Windows - Multiple Failed MSI or Script Applocker Events - Multiple Hosts

Description - is generated if more than one time events with the .msi or script type are generated in a time interval on a multiple hosts. This event will have this error in the message: " was not allowed to run"(the script or .msi file can't run).

AppLocker can help you improve the management of application control and the maintenance of application control policies.

In CYBERQUEST, this alert with 2 Rules will trigger on first event that will match the conditions. To receive the alert information via email, click the following options:



and set



.

Prerequisites - Microsoft-Windows-AppLocker/MSI and Script.

26. Windows - Multiple Failed MSI or Script Applocker Events - Single Host

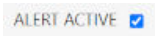
Description - is generated if more than one time events with the .msi or script type are generated in a time interval on a single host. This event will have this error in the message: " was not allowed to run"(the script or .msi file can't run).

AppLocker can help you improve the management of application control and the maintenance of application control policies. In CYBERQUEST, this alert with 2 Rules will trigger on first event that will match the conditions.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - Microsoft-Windows-AppLocker/MSI and Script

27. Windows - Multiple Failed EXE or DLL Applocker Events - Multiple Hosts

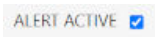
Description - is generated if more than one time events with the .exe or .dll type are generated in a time interval on a multiple hosts. This event will have this error in the message: " was not allowed to run"(the .exe or .dll file can't run.).

AppLocker can help you improve the management of application control and the maintenance of application control policies. In CYBERQUEST, this alert with 2 Rules will trigger on first event that will match the conditions:

To receive the alert information via email, click the following options:



and set



.

Prerequisites - Microsoft-Windows-AppLocker/EXE and DLL

28. Windows - Multiple Failed EXE or DLL Applocker Events - Single Host

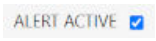
Description - is generated if more than one time events with the .exe or .dll type are generated in a time interval on a single host. This event will have this error in the message: " was not allowed to run"(the .exe or .dll file can't run.).

AppLocker can help you improve the management of application control and the maintenance of application control policies. In CYBERQUEST, this alert with 2 Rules will trigger on first event that will match the conditions.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - Microsoft-Windows-AppLocker/EXE and DLL

29. Windows - BSoD System Crashes on Multiple Hosts

Description - A new event is generated containing details of *BSoD System Crashes on Multiple Hosts*. This alert detects when the system has rebooted without cleanly shutting down first, in a time frame on multiple hosts.

In CYBERQUEST, this alert with 2 Rules will trigger on first event that will match the conditions.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows System Log.

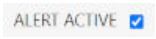
30. Windows - BSoD System Crashes on a Single Host

Description - A new event is generated containing details of *BSoD System Crashes on a Single Host*. This alert detects when the system has rebooted without cleanly shutting down first, in a time frame on a single host.

In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the condition. To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows System Log.

31. Windows - Application Crashes or Hangs on Multiple Hosts

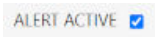
Description - A new event is generated containing details of *Application Crashes or Hangs on Multiple Hosts*. This alert detects the general application error or an application hang, in a time frame on multiple hosts.

In CYBERQUEST, this alert with 2 Rules will trigger on first event that will match the conditions.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows Application Log.

32. Windows - Application Crashes or Hangs on a Single Host

Description - A new event is generated containing details of *Application Crashes or Hangs on a Single Host*. This alert detects the general application error or an application hang in a time frame on a single host.

In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the condition. To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows Application Log.

33. Windows - System or Service Failures on a Single Host

Description - A new event is generated containing details of *System or Service Failures on a Single Host*. Service Control Manager (SCM) stops services and driver services. It also reports when services closes unexpectedly or fail to restart after it takes corrective action.

In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the condition. To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows System Log.

34. Administrator Account logon on 2000-2003-XP

Description - A new event is generated containing details of *Administrator Account logon on 2000-2003-XP*. In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the condition. To receive the alert information via email, click the following options:



and set



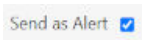
.

Prerequisites - Windows Security Log.

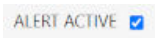
35. Administrator Account Logon on Vista-2008 or Later

Description - A new event is generated containing details of *Administrator Account Logon on Vista-2008 or Later*. This event lets you know whenever an account asssigned any “administrator equivalent” user rights log on.

In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the condition. To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows Security Log.

36. Domain User Failed Logon Due to Invalid Password

Description - A new event is generated when a user fails to logon. The alert is generated when the event is registered with an status and sub-status code and is providing the information: “User logon with misspelled or bad password”.

In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the condition. To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows Security Log.

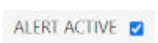
37. Software Uninstalled

Description - A new event is generated when a application has been uninstalled and tell us the name of application and the user account who uninstalled it.

In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the condition. To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows Application Log.

38. New Software Installation

Description - A new event is generated containing details of *New Software Installation*. This event is logged when Windows Installer installed the product.

In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the condition. To receive the alert information via email, click the following options:

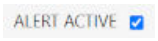
Prerequisites - Windows Application Log.

39. FTP Scan Distinct DestIP

Description - A new event is generated containing details of *File Transfer Protocol Scan Distinct DestIP*. In CYBERQUEST, this alert with 2 Rules will trigger on first event that will match the conditions. To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

40. High data received flow single event

Description - A new event is generated containing details of *High data received flow single event*. In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the condition. To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

41. High data transfered flow single event

Description - A new event is generated containing details of *High data transfered flow single event*. In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the condition. To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

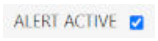
42. User Logon Failed on not allowed computer

Description - A new event is generated containing details of *User Logon Failed on not allowed computer*. The alert is generated when the event is registered with an status and sub-status code and is providing the information: "User logon from an unauthorized workstation".

In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the condition. To receive the alert information via email, click the following options:



and set



.

Prerequisites -Windows Security Log.

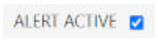
43. User Failed Logon outside his time of day restrictions

Description - A new event is generated containing details of *User Failed Logon outside his time of day restrictions*. The alert is generated when the event is registered with an status and sub-status code and is providing the information: "User logon outside authorized hours".

In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the condition. To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows Security Log.

44. Locked Out Domain Account Failed Logon

Description - A new event is generated containing details of *Locked Out Domain Account Failed Logon*.The alert is generated when the event is registered with an status and sub-status code and is providing the information: "User logon with locked account".

In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the condition. To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows Security Log.

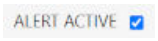
45. Disable Domain Account Failed Logon

Description - A new event is generated containing details of *Disable Domain Account Failed Logon*. The alert is generated when the event is registered with an status and sub-status code and is providing the information: "User logon to account disabled by admin".

In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the condition. To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows Security Log.

46. Domain Account Created

Description - A new event is generated containing details of *Domain Account Created*. When a user account is created in Active Directory, the EventID is logged. This event generates every time a new user object is created.

In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the condition. To receive the alert information via email, click the following options:



and set



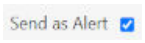
.

Prerequisites - Windows Security Log.

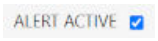
47. Failed Logon Due to Invalid Domain Username

Description - A new event is generated containing details of *Failed Logon Due to Invalid Domain Username*. For this alert the hexadecimal status and sub-status code generated when the event is registered and provide this information: "User logon with misspelled or bad user account".

In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the condition. To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows Security Log.

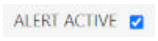
48. Network admin login

Description - A new event is generated containing details of *Network admin login*. The alert is generated if the username is in the administrator list.

In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the condition. To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows Security Log.

49. File Deleted

Description - A new event is generated containing details of *File Deleted*. The alert detects when a file was deleted.

In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the condition. To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows Security Log.

50. SSH Scan Distinct DestIP

Description - A new event is generated if contains a Source IP, Destination IP and Networking default Port (*e.g. SSH Scan default port is 22*).

In CYBERQUEST, this alert with 2 Rules will trigger on first event that will match the conditions. To receive the alert information via email, click the following options:



and set



.

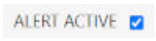
Prerequisites - NetFlow

51. Print Doc Confidential

Description - A new event is generated containing details of *Print Doc Confidential*. In CYBERQUEST, this alert with 2 Rules will trigger on first event that will match the conditions. To receive the alert information via email, click the following options:



and set



.

Prerequisites - Microsoft-Windows-PrintService/Operational.

52. External IP FTP Scan

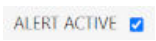
Description - A new event is generated if contains a newtorking protocol, Source IP(from external private networks), Destination IP and a Networking default Port (*e.g. FTP Scan default port is 21*).

File Transfer Protocol (FTP) is a method of transferring files from one computer to another over the Internet.

In CYBERQUEST, this alert with 2 Rules will trigger on first event that will match the conditions. To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

53. VNC Scan

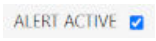
Description - A new event is generated if contains a newtorking protocol, Source IP, Destination IP and a Networking default Port (*e.g. VNC Scan default port is 4900*).

Virtual Network Computing is a graphical desktop-sharing system that uses the Remote Frame Buffer protocol (RFB) to remotely control another computer.

In CYBERQUEST, this alert with 2 Rules will trigger on first event that will match the conditions. To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

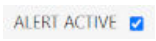
54. PostgreSQL Scan

Description - A new event is generated if contains a newtorking protocol, Source IP, Destination IP and a Networking default Port (*e.g. PostgreSQL Scan default port is 5432*).

In CYBERQUEST, this alert with 2 Rules will trigger on first event that will match the conditions. To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

55. Telnet Scan

Description - A new event is generated if contains a newtorking protocol, Source IP, Destination IP and a Networking default Port (*e.g. Telnet Scan default port is 23*).

Telnet is a network protocol used to virtually access a computer and provide a text-based communication channel between two machines.

In CYBERQUEST, this alert with 2 Rules will trigger on first event that will match the conditions. To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

56. Windows RPC Scan

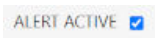
Description - A new event is generated if contains a newtorking protocol, Source IP, Destination IP and a Networking default Port (*e.g. Windows RPC Scan default port is 135*).

Remote Procedure Call is a software communication protocol that one program can use to request a service from a program located in another computer on a network without having to understand the network's details.

In CYBERQUEST, this alert with 2 Rules will trigger on first event that will match the conditions. To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

57. RDP Scan

Description - A new event is generated if contains a newtorking protocol, Source IP, Destination IP and a Networking default Port (*e.g. RDP Scan default port is 3389*).

Remote desktop protocol - is a secure network communications protocol developed by Microsoft. It enables network administrators to remotely diagnose problems that individual users encounter and gives users remote access to their physical work desktop computers.

In CYBERQUEST, this alert with 2 Rules will trigger on first event that will match the conditions. To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

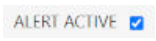
58. MySQL Scan

Description - A new event is generated if contains a newtorking protocol, Source IP, Destination IP and a Networking default Port (*e.g. MySQL Scan default port is 3306*).

In CYBERQUEST, this alert with 2 Rules will trigger on first event that will match the conditions. To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

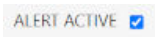
59. MSSQL Scan

Description - A new event is generated if contains a newtorking protocol, Source IP, Destination IP and a Networking default Port (*e.g. MySQL Scan default port is 1433*).

In CYBERQUEST, this alert with 2 Rules will trigger on first event that will match the conditions. To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

60. SSH Scan

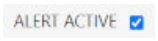
Description - A new event is generated if contains a Source IP, Destination IP and Networking default Port (*e.g. SSH Scan default port is 22*).

Is an prototype SSH configuration and policy scanner for Linux and UNIX servers.

In CYBERQUEST, this alert with 2 Rules will trigger on first event that will match the conditions. To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

61. Event Log Cleared

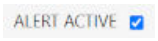
Description - A new event is generated containing details of *Windows Event log cleared*.

In CYBERQUEST, this alert will trigger on the first event that will match the conditions from Windows Event log cleared report. This Report shows if and when the Windows Sercurity Event Log was cleared.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows Security Log.

62. Internal IP FTP Scan

Description - A new event is generated if contains a newtorking protocol, Source IP (from internal private networks), Destination IP and a Networking default Port (*e.g. FTP Scan default port is 21*).

File Transfer Protocol (FTP) is a method of transferring files from one computer to another over the Internet.

In CYBERQUEST, this alert with 2 Rules will trigger on first event that will match the Conditions. To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

63. ICMP Scan

Description - A new event is generated containing details of *ICMP Scan*. Internet Control Message Protocol requests are used to map network topology. Receipt of an ICMP request is classified as a normal, possibly suspicious, or highly suspicious event.

In CYBERQUEST, this alert with 2 Rules will trigger on first event that will match the Conditions. To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

64. VPN Geographic Impossible Traveling

Description - A new event is generated containing details of *VPN Geographic Impossible Traveling*.

In CYBERQUEST, this alert with 2 Rules will trigger on first event that will match the Conditions. To receive the alert information via email, click the following options:



and set



.

Prerequisites - FortiGate

65. Malware Detection

Description - A new event is generated containing details of *Malware Detection*. Malware detection refers to the process of detecting the presence of malware on a host system or of distinguishing whether a specific program is malicious.

In CYBERQUEST, this alert with 2 Rules will trigger on first event that will match the Conditions. To receive the alert information via email, click the following options:



and set



.

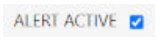
Prerequisites - FortiGate

66. Network Intrusion Detection

Description - A new event is generated containing details of *UTM > IPS > Alert*. In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the Condition. To receive the alert information via email, click the following options:



and set



.

Prerequisites - FortiGate

67. FortiGate UTM-WAF High Severity Level

Description - A new event is generated containing details of *Traffic High Reputation Level*. In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the Condition. To receive the alert information via email, click the following options:



and set



.

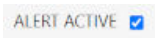
Prerequisites - FortiGate

68. Domain OR Enterprise Admins Modification

Description - A new event is generated containing details of *Group Modification*. In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the Condition. To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows Security Log.

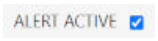
69. Network DoS

Description - A new event is generated containing details of *Network DoS*. A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users.

In CYBERQUEST, this alert with 2 Rules will trigger on first event that will match the Conditions. To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

70. Network DDoS on Other Protocol

Description - A new event is generated containing details of *Network DDoS on Other Protocol*. In CYBERQUEST, this alert with 2 Rules will trigger on first event that will match the Conditions.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

71. Network DDoS on ICMP Protocol

Description - A new event is generated containing details of *Network DDoS on ICMP Protocol*. In CYBERQUEST, this alert with 2 Rules will trigger on first event that will match the Conditions.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

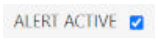
72. Network DDoS on TCP Protocol

Description - A new event is generated containing details of *Network DDoS on TCP Protocol*. In CYBERQUEST, this alert with 2 Rules will trigger on first event that will match the Conditions.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

73. Network DDoS on UDP Protocol

Description - A new event is generated containing details of *Network DDoS on UDP Protocol*. In CYBERQUEST, this alert with 2 Rules will trigger on first event that will match the Conditions.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

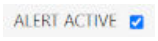
74. High dataTransfer flow

Description - A new event is generated containing details of *High dataTransfer flow*. In CYBERQUEST, this alert with 2 Rules will trigger on first event that will match the Conditions.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

75. 3 failed SU password for root

Description - A new event is generated containing details of *3 failed SU password for root*. In CYBERQUEST, this alert with 2 Rules will trigger on first event that will match the Conditions.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - syslog

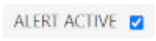
76. Unable to log events to Windows Security

Description - A new event is generated containing details of *Unable to log events to Windows Security*. The event is logged if Windows was unable to write events to the Security event log.

In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the Condition. To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows Security Log.

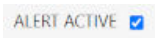
77. A security-enabled universal group was changed

Description - A new event is generated containing details of *A security-enabled universal group was changed*. When a universal security group is changed in Active Directory, the EventID gets logged.

In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the Condition. To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows Security Log.

78. A security-enabled universal group was created

Description - A new event is generated containing details of *A security-enabled universal group was created*. When a universal security group is created in Active Directory, the EventID gets logged.

In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the Condition. To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows Security Log.

79. A security-enabled global group was changed

Description - A new event is generated containing details of *A security-enabled global group was changed*. When a universal security group is changed in Active Directory, the EventID gets logged.

In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the Condition. To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows Security Log.

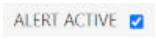
80. A security-enabled local group was changed

Description - A new event is generated containing details of *A security-enabled local group was changed*. The event generates every time a security-enabled local group is changed.

In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the Condition. To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows Security Log.

81. A security-enabled local group was deleted

Description - A new event is generated containing details of *A security-enabled local group was deleted*. The event generates every time a security-enabled local group is deleted.

In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the Condition. To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows Security Log.

82. A member was removed to a AD Local Group

Description - A new event is generated containing details of *A member was removed to a AD Local Group*. The event generates every time member was removed from a security-enabled local group.

In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the Condition. To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows Security Log.

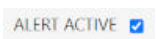
83. A member was added to a AD Local Group

Description - A new event is generated containing details of *A member was added to a AD Local Group*. The event generates every time member was added to a security-enabled local group.

In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the Condition. To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows Security Log.

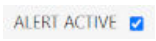
84. A security-enabled global group was created

Description - A new event is generated containing details of *A security-enabled global group was created*. When a security-enable global group is created in Active Directory, the EventID gets logged.

In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the Condition. To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows Security Log.

85. User Added/Removed from AD Global Group

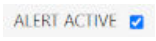
Description - A new event is generated containing details of *User Added/Removed from AD Global Group*. When Active Directory objects such as an user/group/computer is added or removed to a security global group, the EventID gets logged.

In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the Condition.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows Security Log.

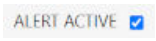
86. A security-enabled local group was created

Description - A new event is generated containing details of *User Added or Removed from Security-Enabled Global Admins Group*. The event generates every time a security-enabled local group was created.

In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the Condition. To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows Security Log.

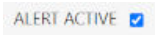
87. A security-enabled global group was deleted

Description - A new event is generated containing details of *A security-enabled global group was deleted*. In Active Directory, when a Security Global Group is deleted, the EventID gets logged.

In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the Condition. To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows Security Log.

88. User Added/Removed from AD Global Admins Group

Description - A new event is generated containing details of *User Added or Removed from Security-Enabled Global Admins Group*. When Active Directory objects such as an user/group/computer is added or removed to a security global admins group, the EventID gets logged.

In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the Condition. To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows Security Log.

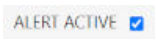
89. Windows Authentication Brute Force same UserName And Computer

Description - A new event is generated containing details of *Windows Authentication Brute Force same UserName And Computer*. In CYBERQUEST, this alert with 2 Rules will trigger on first event that will match the Conditions.

To receive the alert information via email, click the following options:



and set



.

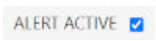
Prerequisites - Windows Security Log.

90. ROOT authentication failure

Description - A new event is generated containing details of *Invalid user*. In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the Condition. To receive the alert information via email, click the following options:



and set



.

Prerequisites - syslog

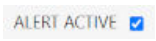
91. VPN Login and RDP with another UserName

Description - A new event is generated containing details of *VPN Login and RDP with another UserName*. In CYBERQUEST, this alert with 2 Rules will trigger on first event that will match the Conditions.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - syslog

92. Authorization policy change

Description - A new event is generated containing details of *Authorization policy change*. Audit Authentication Policy Change determines whether the operating system generates audit events when changes are made to authentication policy. Events list for this alert:

- Permissions on an object were changed
- A new trust was created to a domain
- A trust to a domain was removed
- Trusted domain information was modified
- Kerberos policy was changed
- System security access was granted to an account
- System security access was removed from an account
- Domain Policy was changed
- A namespace collision was detected
- A trusted forest information entry was added
- A trusted forest information entry was removed
- A trusted forest information entry was modified

In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the Condition. To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows Security Log.

93. Active Directory Domain Policy modified

Description - A new event is generated containing details of *Active Directory Domain Policy modified*. The event generates when one of the following changes was made to local computer security policy:

- *Computer's "|Security Settings|Account Policies|Account Lockout Policy"* settings were modified.
- *Computer's "|Security Settings|Account Policies|Password Policy"* settings were modified.
- *"Network security: Force logoff when logon hours expire"* group policy setting was changed.

In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the Condition. To receive the alert information via email, click the following options:



and set



.

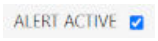
Prerequisites - Windows Security Log.

94. Drop table or database alert

Description - A new event is generated containing details of *Drop table or database alert*. In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the Condition. To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows Application Log.

95. Blacklist IP Alert

Description - A new event is generated containing details of *Blacklist IP Alert*. Detects all the events which contains a SourceIP and DestIP from the BlackList.

In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the Condition. To receive the alert information via email, click the following options:



and set



.

Prerequisites - Network Communications

96. Linux authentication failure

Description - A new event is generated containing details of *Linux authentication failure*. In CYBERQUEST, this alert with 2 Rules will trigger on first event that will match the Conditions.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - syslog

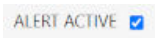
97. Audit policy change

Description - A new event is generated containing details of *Audit policy change*. This event generates when the computer's audit policy changes.

In CYBERQUEST, this alert with 1 Rule will trigger on first event that will match the Condition. To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows Security Log.

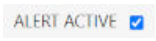
98. Succesful Login After Multiple Fails

Description - A new event is generated containing details of *Succesful Login After Multiple Fails*. In CYBERQUEST, this alert with 3 Rules will trigger on first event that will match the Conditions.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows Security Log.

99. DDOS

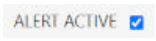
Description - A new event is generated containing details of *DDOS*. DDoS Attack means "Distributed Denial-of-Service (DDoS) Attack" and it is a cybercrime in which the attacker floods a server with internet traffic to prevent users from accessing connected online services and sites.

In CYBERQUEST, this alert with 2 Rules will trigger on first event that will match the Conditions.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

100. Suspicious RDP Connection Success

Description - this alert indicates a successful Remote Desktop Protocol (RDP) connection with suspicious attributes. RDP is commonly used to remotely access systems or servers, and when connections occur unexpectedly or under unusual circumstances, they may represent a security threat. RDP connections are often targeted by brute-force attacks, exploitation of vulnerabilities, or unauthorized access to sensitive systems.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows Security Log

100. Suspicious RDP Connection Failed

Description - identifies Remote Desktop Protocol (RDP) connection attempts originating from potentially unsafe, unrecognized, or high-risk geographic locations. The purpose is to detect unauthorized access attempts, often indicative of brute-force attacks, credential theft, or reconnaissance by threat actors.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows Security Log

101. Recon - Horizontal Telnet Scan: Events or Flows

Description - triggered when a single IP tries to connect via Telnet to multiple internal devices. Trigger if over 5 Telnet attempts from a single IP are detected to different IPs. Port 23

To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

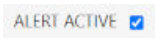
102. Recon - Horizontal SSH Scan: Events or Flows

Description - triggered when multiple SSH connection attempts are made from a single IP to various destinations, indicating an SSH brute-force or discovery attempt. If over 5 SSH attempts to different hosts are observed within 5 minutes.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

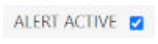
103. Recon - Horizontal SNMP Scan: Events or Flows

Description - triggered when an IP makes multiple SNMP requests across various internal devices, possibly searching for misconfigured SNMP services.Trigger if more than 5 SNMP queries are sent to different IPs. Port 161 and 162.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

104. Recon - Horizontal SMTP Scan: Events or Flows

Description - an IP makes multiple SMTP connection attempts across different internal IPs, indicating potential spam relay discovery or vulnerability probing. If more than 5 SMTP connection attempts to different hosts occur within a short timeframe.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

105. Recon - Horizontal SMB Scan: Events or Flows

Description - triggered when multiple SMB connection attempts are detected from a single IP across different destination IPs, potentially indicating a scan for vulnerable SMB services. Trigger if over 10 SMB connection attempts are made from a single source IP to different destination IPs within a 3 minutes.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

106. Recon - Horizontal RPC Scan: Events or Flows

Description - this alert detects when multiple hosts are targeted via Remote Procedure Call (RPC) services, usually to identify systems with exposed RPC ports.Trigger if multiple connections from one IP to port 135, 593 (RPC) across multiple hosts.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

107. Recon - Horizontal RDP Scan: Events or Flows

Description - alerts when an attacker scans multiple hosts for open RDP (Remote Desktop Protocol) ports, typically port 3389. Trigger on 5+ RDP connection attempts within 5 minutes from a single source IP to multiple destination IPs.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

108. Recon - Horizontal NetBIOS Scan: Port 139: Events and Flows

Description - detects potential lateral movement or scanning of SMB services on port 139 (NetBIOS Session Service). Trigger if the same IP sends packets to port 139 on different internal hosts within a short period.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

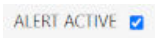
109. Recon - Horizontal NETBIOS Scan: Port 137 and 138

Description - this alert detects multiple NETBIOS queries on ports 137 and 138, commonly used for network discovery and potential SMB-related attacks. Trigger if multiple connections are made to NETBIOS ports (137/138) from a single IP across different hosts.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

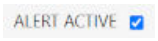
110. Recon - Horizontal HTTPS Scan: Events or Flows

Description - this alert is generated when HTTPS traffic is being scanned across multiple internal hosts.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

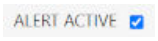
111. Recon - Horizontal HTTP Scan: Events or Flows

Description - triggered when multiple HTTP requests are detected from a single host across different IP addresses, indicative of a scan for open HTTP ports.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

112. CiscoASA - No matching connection for ICMP error message

Description - triggers when an ICMP (Internet Control Message Protocol) error message is detected without a corresponding initial connection. Normally, ICMP error messages, like “Destination Unreachable” or “Time Exceeded,” are responses to previously sent network packets. When these error messages appear without an initiating connection, it can indicate several potential issues, such as packet spoofing, malicious scanning, or routing misconfigurations.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - CiscoASA

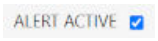
113. Checkpoint DROP From Blocked IP By Country

Description - identifies when a Check Point firewall drops traffic originating from IP addresses in countries that are blocked based on organizational policy or threat intelligence feeds. The alert is designed to monitor and flag incoming traffic from high-risk or geopolitically restricted regions.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - Checkpoint

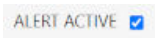
114. New USB Detected

Description - this alert indicates that a USB device has been connected to a monitored system. USB devices can be used for various purposes, but they also represent a security risk, as they can be used to transfer unauthorized files, introduce malware, or steal sensitive data.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows Security Log

115. Web Filter - Excessive Web Connections

Description - set a rule to count the number of web connections (HTTP/HTTPS) initiated by a user or an IP address within a specific time frame (e.g., 5 minutes). The specific threshold may vary depending on the network, but generally, it defines a maximum number of allowed connections within a given period (e.g., 100 connections in a 5-minute window).

To receive the alert information via email, click the following options:



and set



.

Prerequisites - Fortigate

116. Web Filter - Multiple Blocked Web Policy Connections

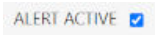
Description - Monitor the traffic on ports 80 (HTTP) and 443 (HTTPS) to track attempts to access blocked websites. Identify the same SrcIP within a 2-minute interval or 5-10 attempts to access blocked sites.

This alert indicates that a user, device, or application has attempted to access a significant number of websites or resources that are blocked according to the organization's web filtering policy. This behavior may signal unintentional activities, unauthorized access, or potentially malicious intent.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - Fortigate

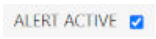
117. Recon - Multiple UDP Recon Events from a Remote Host

Description - Monitors for UDP-based reconnaissance. Indicators: Probing of open UDP ports (e.g., DNS, SNMP, NTP). Excessive traffic from a single source. Threshold: >30 UDP packets in 5 minutes.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

118. Recon - Multiple UDP Recon Events from a Local Host

Description - Monitors for UDP-based reconnaissance. Indicators: Probing of open UDP ports (e.g., DNS, SNMP, NTP). Excessive traffic from a single source. Threshold: >40 UDP packets targeting multiple ports in 5 minutes.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

119. Recon - Multiple TCP Recon Events from a Remote Host

Description - Identifies TCP-based port scans or probing. Indicators: SYN packets without completed handshakes. Sequential connection attempts to multiple ports. Threshold:>30 connection attempts in 5 minutes.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

120. DNS - Communication with Malicious Host - Event or Flow

Description - A device within internal network, such as a computer, server, or any networked device, initiating communication with a known malicious host via DNS queries.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

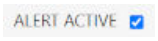
121. GTI Communication with Malicious Host _Event _FortiGate

Description - Communication detected between a local device and a host identified as malicious by Global Threat Intelligence (GTI) sources, based on logs from FortiGate firewall.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - FortiGate

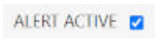
122. DNS - Local Host Communicating with External DNS Server - Flow

Description - Indicates that a local host within your network is communicating with an external DNS server.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

123. DNS - Multiple Recon Events from a Local Host

Description - A local host from internal network is performing multiple reconnaissance (recon) events through DNS queries. Reconnaissance is a technique used to gather information about a network, systems, or services to identify potential vulnerabilities. Multiple recon events suggest that the local host is systematically probing the network

To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

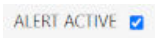
124. DNS - Multiple Recon Events from a Remote Host

Description - A remote host is performing multiple reconnaissance (recon) events through DNS queries.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

125. DNS - Possible DNS Amplification Attack

Description - A Distributed Denial of Service (DDoS) attack type where an attacker exploits the functionality of open DNS resolvers to flood a target with an overwhelming amount of traffic: The attacker sends DNS queries with a spoofed IP address (the target's IP) to a vulnerable DNS server. The server responds to these queries, amplifying the volume of traffic sent to the target. Open DNS Resolver: A DNS server that responds to queries from any IP address, often exploited in amplification attacks. Spoofed IP Address: The attacker falsifies the source IP address in DNS requests, making it appear as if the target IP is requesting information.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

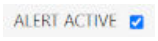
126. IPS Events

Description - Pertains to events detected by an Intrusion Prevention System (IPS)-a network security device or software that monitors network traffic for suspicious activity and takes immediate action to prevent potential threats from causing harm.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - CheckPointFirewall

127. Virus detected

Description - A virus has been detected on a device within the network, using Gdata Antivirus.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - Antivirus Gdata

128. AD blocked users

Description - A user account in Active Directory (AD) has been blocked or locked out. This typically happens due to multiple failed login attempts, policy violations, or manual administrative actions.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows Security Log

129. DNS - Data Exfiltration Detection

Description - Unauthorized transfer of data from a computer or network: unusual volumes of data being transferred, especially during off-hours; data being sent to unknown or unauthorized external IP addresses; usage of uncommon protocols or ports for data transfer; repeated or large data transfers to cloud storage services or external servers.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

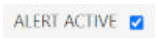
131. Exfiltration - FTP Traffic with High-Value Host

Description - Indicates that FTP (File Transfer Protocol) traffic involving a high-value host has been detected, which may be a sign of data exfiltration. This type of alert is important because FTP is often used to transfer files between systems, and when it involves a high-value host, it may indicate that sensitive or critical data is being improperly transferred.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

132. Exfiltration - IM Client File Transfers with High-Value Hosts

Description - Detect file transfers via instant messaging (IM) clients on high value hosts.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

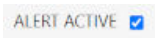
133. Exfiltration - P2P Activity with High-Value Hosts

Description - Detect file transfers via instant messaging (IM) clients on high value hosts.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - Fortigate

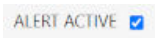
134. GData - Detected WebPhishing

Description - This alert indicates that the GData security solution has detected a phishing attempt through a website accessed by a user or a connection containing a malicious URL. The phishing site is designed to steal sensitive information, such as authentication credentials, financial details, or other personal data, by deceiving the user.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - GData

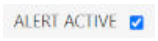
135. Exfiltration - High Number of File Status Events on High-Value Hosts

Description - Unusually high number of file status events (such as file creations, deletions, modifications, or movements) occurring on high-value hosts. High-value hosts are systems that hold critical or sensitive data, making them prime targets for attackers

To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows File Access

136. GData - Detected WebInfection

Description - This alert indicates that the GData security solution has identified a web infection, suggesting the possibility of a compromised website or a malicious download. The device may have accessed infected content or fallen victim to a drive-by download attack, where malicious code is executed without the user's knowledge.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - GData

137. Administrator Account Locked

Description - A administrator account in Active Directory (AD) has been blocked or locked out. This typically happens due to multiple failed login attempts, policy violations, or manual administrative actions.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows Security Log

138. A user account was locked out

Description - A user account in Active Directory (AD) has been blocked or locked out. This typically happens due to multiple failed login attempts, policy violations, or manual administrative actions.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows Security Log

139. A user account was locked out

Description - A user account in Active Directory (AD) has been blocked or locked out. This typically happens due to multiple failed login attempts, policy violations, or manual administrative actions.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows Security Log

140. FortiGate Torrent Activity Detected

Description - Indicates that the FortiGate firewall has detected torrent activity within the network.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - Fortigate

141. Forti High Traffic from single IP

Description - A single IP address is generating an unusually high volume of network traffic.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - Fortigate

142. Possible Malicious File By Filename Match

Description - A single IP address is generating an unusually high volume of network traffic.

To receive the alert information via email, click the following options:



and set



.

143. Fortigate - Malware - Botnet Activity

Description - Triggered when a FortiGate device identifies network traffic indicative of botnet activity. Botnets are collections of compromised devices under the control of an attacker, often used for malicious purposes such as DDoS attacks, spamming, data theft, or lateral movement within a network.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - Fortigate

144. FortiGate update failed

Description - Triggered when a FortiGate device fails to complete a firmware update, pattern update, or feature upgrade. Such failures can indicate potential issues with system functionality, network security, or communication between the FortiGate and update servers.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - Fortigate

145. CiscoASA - SSH Admin Login

Description - An administrative login has been detected on the Cisco ASA device using the SSH protocol. This event indicates an attempt to access the device for management purposes. Ensure the activity is authorized and aligns with operational policies.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - CiscoASA

146. CiscoASA - TELNET Admin Login

Description - An administrative login attempt has been detected on the Cisco ASA device using the Telnet protocol. Since Telnet transmits data unencrypted, this activity should be reviewed for compliance and security risks.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - CiscoASA

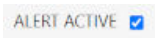
147. CiscoASA - HTTPS Admin Login

Description - An administrative login was detected on the Cisco ASA device using the HTTPS protocol. Ensure the access was authorized and verify that the connection is secure.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - CiscoASA

148. CiscoASA - A new username was created

Description - A new administrative username has been created on the Cisco ASA device. This action may indicate routine administrative activity or potential unauthorized changes. Verify the legitimacy of this account creation.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - CiscoASA

149. CiscoASA - A new username was deleted

Description - An existing administrative username has been deleted on the Cisco ASA device. This action could indicate routine administrative cleanup or an attempt to remove traces of unauthorized access. Investigate as needed.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - CiscoASA

150. Recon - DNS Recon Events from a Local Host

Description - Detects anomalous DNS queries originating from a local host, indicating potential subdomain enumeration or DNS reconnaissance activity. Indicators: Large number of DNS queries in a short time. Queries to non-corporate or suspicious domains. Repeated queries with incremental subdomain changes (e.g., a.example.com, b.example.com). Threshold: >50 DNS queries to different domains or subdomains within 10 minutes.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

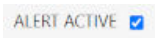
151. Recon - DNS Recon Events from a Remote Host

Description - Identifies DNS recon attempts from an external source targeting internal infrastructure. Indicators: Queries aimed at internal domain names. High-frequency requests from a single IP address. Threshold: >30 queries from a single external IP to internal domains in 5 minutes.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

152. Recon - MySQL/MariaDB Database Recon Events from a Local Host

Description - Monitors local activity for database enumeration or brute force attempts on MySQL/MariaDB. Indicators: Failed login attempts. Use of commands like SHOW DATABASES, SHOW TABLES. Threshold: >5 failed logins or enumeration commands in 5 minutes.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

153. Recon - PostgreSQL Database Recon Events from a Local Host

Description - Tracks PostgreSQL-specific recon or enumeration activities locally. Indicators: Commands such as \l (list databases), \dt (list tables). Failed connection attempts. Threshold: >3 enumeration commands or failed logins in 5 minutes.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

154. Recon - Microsoft SQL Server Database Recon Events from a Local Host

Description - Identifies local recon attempts targeting MSSQL. Multiple failed logins. Threshold: >10 recon queries or failed login attempts within 10 minutes.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

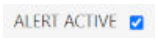
155. Recon - MySQL/MariaDB Database Recon Events from a Remote Host

Description - Monitors remote attempts to probe MySQL/MariaDB databases. Indicators: Network connections from external IPs attempting to access database ports (3306). Enumeration commands detected. Threshold: >10 attempts to access MySQL from a remote source in 5 minutes.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

156. Recon - PostgreSQL Database Recon Events from a Remote Host

Description - Tracks external recon activity against PostgreSQL. Indicators: Unauthorized connection attempts. Use of PostgreSQL-specific commands from external IPs. Threshold: >10 connection attempts or enumeration commands from a remote host in 10 minutes.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

157. Recon - Microsoft SQL Server Database Recon Events from a Remote Host

Description - Detects MSSQL recon activity originating from remote sources. Indicators: Connection attempts to default MSSQL port (1433). Failed logins combined with recon commands. Threshold: >15 unauthorized attempts within 10 minutes.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

158. Recon - MySQL/MariaDB Database Multiple Recon Events from a Local Host

Description - Indicates that multiple scanning or reconnaissance (recon) events targeting MySQL/MariaDB databases have been detected originating from a local host.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

159. Recon - PostgreSQL Database Multiple Recon Events from a Local Host

Description - Detects MSSQL recon activity originating from remote sources. Indicators: Connection attempts to default MSSQL port (1433). Failed logins combined with recon commands. Threshold: >15 unauthorized attempts within 10 minutes.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

160. Recon - Microsoft SQL Server Database Multiple Recon Events from a Local Host

Description - Indicates that a local device on the network has made multiple scanning or access attempts toward a Microsoft SQL Server database.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

161. Recon - Oracle Database Multiple Recon Events from a Local Host

Description - Indicates the detection of multiple reconnaissance activities targeting an Oracle database, initiated by a host within the local network.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

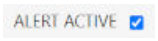
162. Recon - MySQL/MariaDB Database Multiple Recon Events from a Remote Host

Description - Indicates that multiple reconnaissance events targeting MySQL/MariaDB databases have been detected, originating from a remote host.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

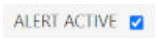
163. Recon - PostgreSQL Database Multiple Recon Events from a Remote Host

Description - Indicates multiple reconnaissance events targeting a PostgreSQL database from an external location. Reconnaissance is the process by which an attacker or external user gathers information about the database structure, users, permissions, or software versions to identify potential vulnerabilities that could later be exploited.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

164. Recon - Microsoft SQL Server Database Multiple Recon Events from a Remote Host

Description - Indicates the detection of multiple reconnaissance events conducted by an external host targeting a Microsoft SQL server within the network

To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

165. Recon - Oracle Database Multiple Recon Events from a Remote Host

Description - Signals the detection of multiple reconnaissance events conducted by an external host targeting a Microsoft SQL server within the network.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

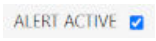
166. Recon - FTP Recon Events from a Local Host

Description - Tracks local probing activity against FTP servers. Indicators: Repeated login attempts (successful or failed). Directory enumeration commands (e.g., LIST, NLST). Threshold: >5 login attempts or >10 directory commands in 5 minutes.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

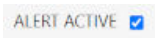
167. Recon - FTP Recon Events from a Remote Host

Description - Identifies remote FTP recon activity. Indicators: Connections to FTP ports (21). Login brute force attempts. Threshold: >10 login attempts or >20 enumeration commands in 10 minutes.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

168. Recon - FTP Multiple Recon Events from a Local Host

Description - Indicates the detection of multiple reconnaissance (recon) events via the FTP (File Transfer Protocol) by a local host within the network. These activities involve repeated access attempts, directory listings, or resource identification on FTP servers, which could suggest an attempt to map available FTP services in the network.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

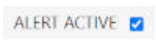
169. Recon - FTP Multiple Recon Events from a Remote Host

Description - Indicates the detection of multiple reconnaissance activities targeting the FTP (File Transfer Protocol) service from an external host.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

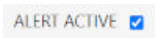
170. Recon - Multiple ICMP Recon Events from a Remote Host

Description - Detects ICMP reconnaissance activity like ping sweeps or path discovery. Indicators: Multiple ICMP echo requests in quick succession. ICMP requests targeting restricted or sensitive segments. Threshold: >30 ICMP packets in 5 minutes.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

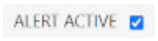
171. Recon - Multiple ICMP Recon Events from a Local Host

Description - Detects ICMP reconnaissance activity like ping sweeps or path discovery. Indicators: Multiple ICMP echo requests in quick succession. ICMP requests targeting restricted or sensitive segments. Threshold:>50 ICMP packets in 5 minutes.

To receive the alert information via email, click the following options:



and set



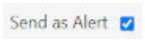
.

Prerequisites - NetFlow

172. Recon - Multiple TCP Recon Events from a Local Host

Description - Identifies TCP-based port scans or probing. Indicators: SYN packets without completed handshakes. Sequential connection attempts to multiple ports. Threshold: >50 connection attempts in 5 minutes.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

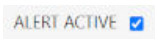
173. Forti Admin Session

Description - Admin login successful, admin logout successful - minimum 1, maximum 30 in 600 seconds identifies admin login events and checks if other types of events have occurred as well.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - Fortigate

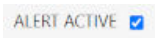
174. Recon - Oracle Database Recon Events from a Remote Host

Description - Monitors remote recon or probing of Oracle databases. Indicators: Attempts to access Oracle listener ports (1521). Enumeration commands executed by external IPs. Threshold: >10 access attempts or queries from a single external source in 10 minutes.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

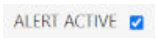
175. User Added/Removed from AD Global Admins Group

Description - Indicates that a user has been added or removed from the Global Admins group in Active Directory (AD). Any changes to this group are highly sensitive and can have significant implications for the security and integrity of the organization.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - Windows Security Log

176. VPNSuccess - from outside Romania

Description - Indicates a successful VPN authentication from a geographic location outside of Romania. This could represent legitimate activity if the user is traveling or working remotely, but it may also signal a potential security breach, especially if access from other countries is unusual for the organization.

To receive the alert information via email, click the following options:



and set



.

177. Forti Admin Login successful

Description - Indicates that a user has successfully authenticated on a FortiGate device using an administrative account (admin).

To receive the alert information via email, click the following options:



and set



.

Prerequisites - Fortigate

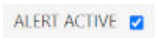
178. VPNFailed - from outside Romania

Description - Indicates a failed VPN connection attempt to the organization's network from a location outside of Romania. This type of event may signal unauthorized access attempts, the use of compromised credentials, or incorrect user configurations.

To receive the alert information via email, click the following options:



and set



.

179. VPNSuccess - from User Not in WindowsUserList

Description - Indicates that a user who is not present in the Windows User List (WindowsUserList) has successfully authenticated into the network via VPN.

To receive the alert information via email, click the following options:



and set



.

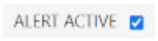
180. Recon - Oracle Database Recon Events from a Local Host

Description - Detects enumeration or login attempts targeting Oracle databases locally. Repeated login failures. Threshold: >5 recon-related commands or failed logins in 5 minutes.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - NetFlow

181. Forti Admin login failed

Description - Indicates a failed authentication attempt on the administrative interface of a Fortinet FortiGate device.

To receive the alert information via email, click the following options:



and set



.

Prerequisites - Fortigate

Vulnerabilities

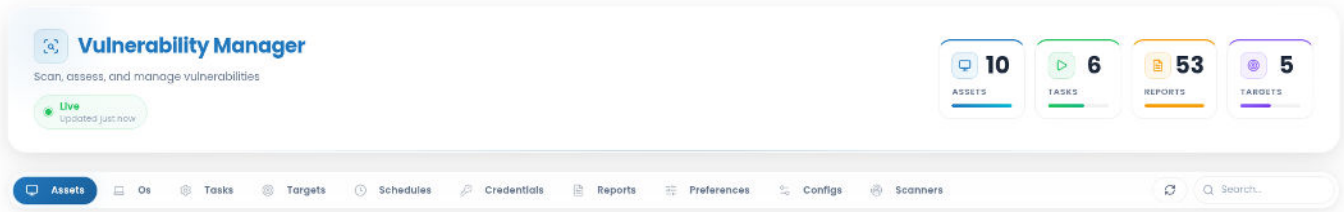
Overview

Vulnerability Manager

The **Vulnerability Manager** module allows users to scan, assess, and manage vulnerabilities identified across infrastructure assets. CYBERQUEST integrates with **OpenVAS** (https://www.openvas.org/) (https://www.openvas.org/%29), a vulnerability scanner used to detect vulnerabilities, exposed services, misconfigurations, and other security-relevant findings.

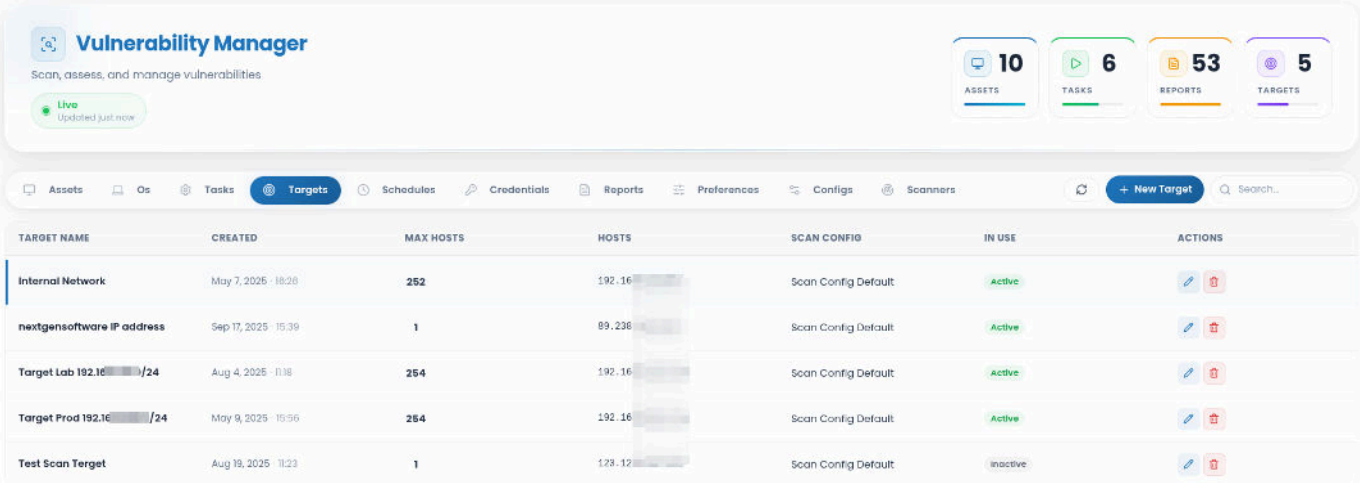
The scanner uses vulnerability tests from an updated feed, allowing new detection checks to be applied as they become available.

The **Vulnerability Manager** provides access to the main components required to configure and run vulnerability scans, including **Assets**, **OS**, **Tasks**, **Targets**, **Schedules**, **Credentials**, **Reports**, **Preferences**, **Configs**, and **Scanners**.



Targets

Before a vulnerability scan can be executed, one or more scan targets must be defined. A target specifies the hosts that will be scanned and the credentials or scanning options that should be used.



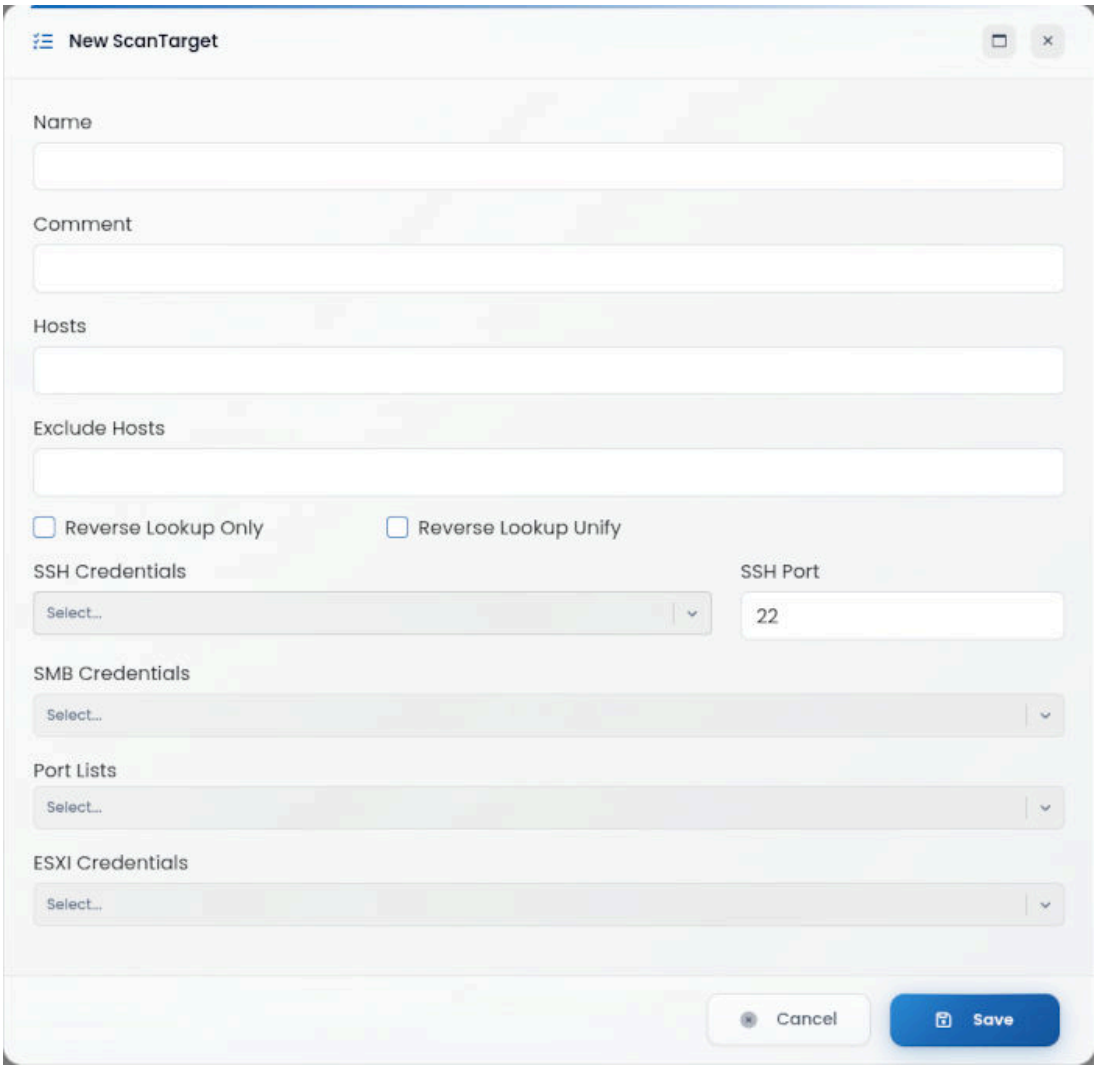
Available actions include:

- **Edit targets** - Modifies an existing scan target configuration.
- **Delete targets** - Removes the selected scan target. This action is irreversible and requires confirmation.

To create a new scan target, click the



button:



The following fields are available:

Name: Defines a unique name for the scan target.

Comment: Provides optional notes or details about the target.

Hosts: Specifies the hosts to be scanned. This field supports IP addresses, hostnames, comma-separated values, hyphenated ranges, or CIDR notation.

Exclude Hosts: Defines hosts that must be excluded from the scan.

- *Reverse Lookup Only*: Enables reverse DNS lookup for the specified hosts.
- *Reverse Lookup Unify*: Normalizes and groups reverse lookup results.

SSH Credentials:Selects the credentials used for SSH authentication.

SSH Port: Defines the SSH port used during authenticated scanning. The default value is `22`

SMB Credentials: Selects the credentials used for SMB authentication.

Port Lists: Selects the port profile used during scanning.

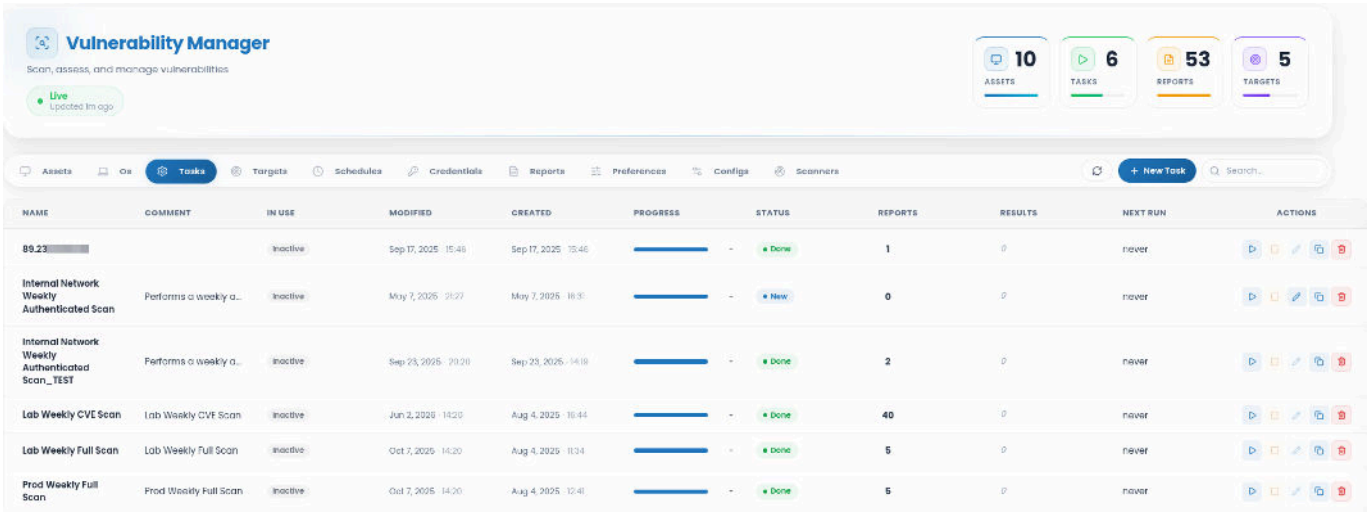
- All IANA assigned TCP
- All IANA assigned TCP and UDP
- All TCP and Nmap top 100 UDP

ESXI Credentials: Selects credentials used for ESXi systems, if applicable.

After completing the required fields, click **Save** to create the target.

Tasks

The **Tasks** section defines the actual vulnerability scan jobs. A task combines the scan target, scan configuration, scanner engine, schedule, and execution options.



- **Start task**

  - Starts the selected scan task manually.

- **Stop task**

  - Stops a running scan task.

- **Edit task**

  - Modifies the selected scan task.

- **Clone task**

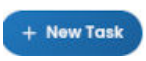
  - Creates a copy of an existing task.

- **Delete tasks**

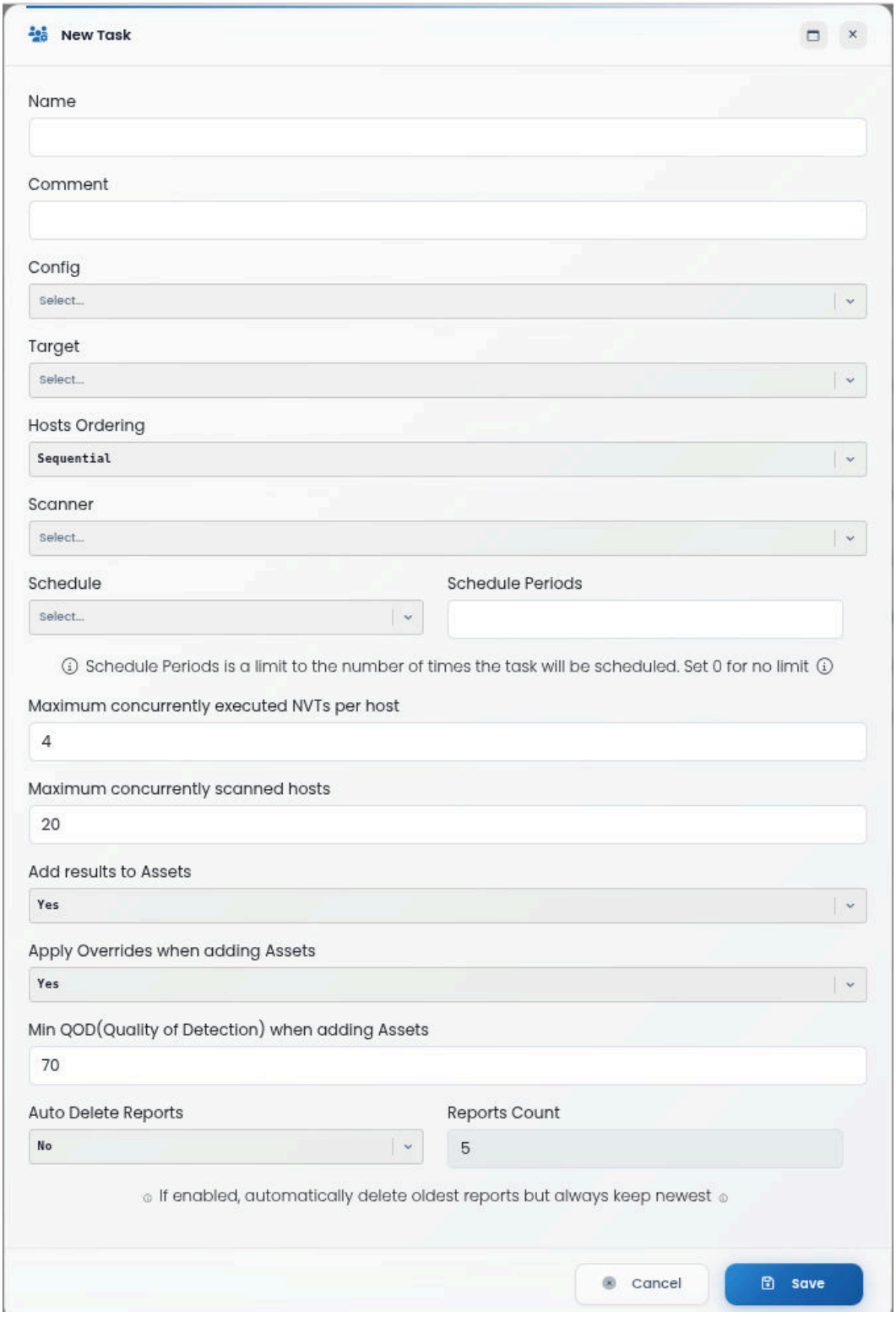
  

  - Removes the selected task and associated data, where applicable. This action requires confirmation.

To create a new task, click the



button.



The following fields are available:

Name: Defines the task name.

Comment: Provides optional information about the task.

Config: Selects the scan configuration profile used by the task.

Target: Selects the target hosts to be scanned.

Hosts Ordering: Defines the order in which hosts are scanned.

- **Sequential**: Scans hosts in the listed order.
- **Random**: Scans hosts in random order.

- **Reverse**: Scans hosts in reverse order.

Scanner: Selects the scanner engine used for the task.

Schedule: Selects a predefined schedule for automatic execution.

Schedule Periods: Defines how many times the task should run according to the selected schedule. A value of `0` means no execution limit.

Maximum concurrently executed NVTs per host: Defines the maximum number of Network Vulnerability Tests that can run at the same time on each host.

Maximum concurrently scanned hosts: Defines how many hosts can be scanned in parallel.

Add results to Assets: Enables or disables adding scan results to the asset inventory.

Apply Overrides when adding Assets:Enables or disables applying overrides when adding scan results to assets.

Min QOD (Quality of Detection) when adding Assets: Defines the minimum QoD value required for results to be added to asset records.

Auto Delete Reports: Enables or disables automatic deletion of older reports.

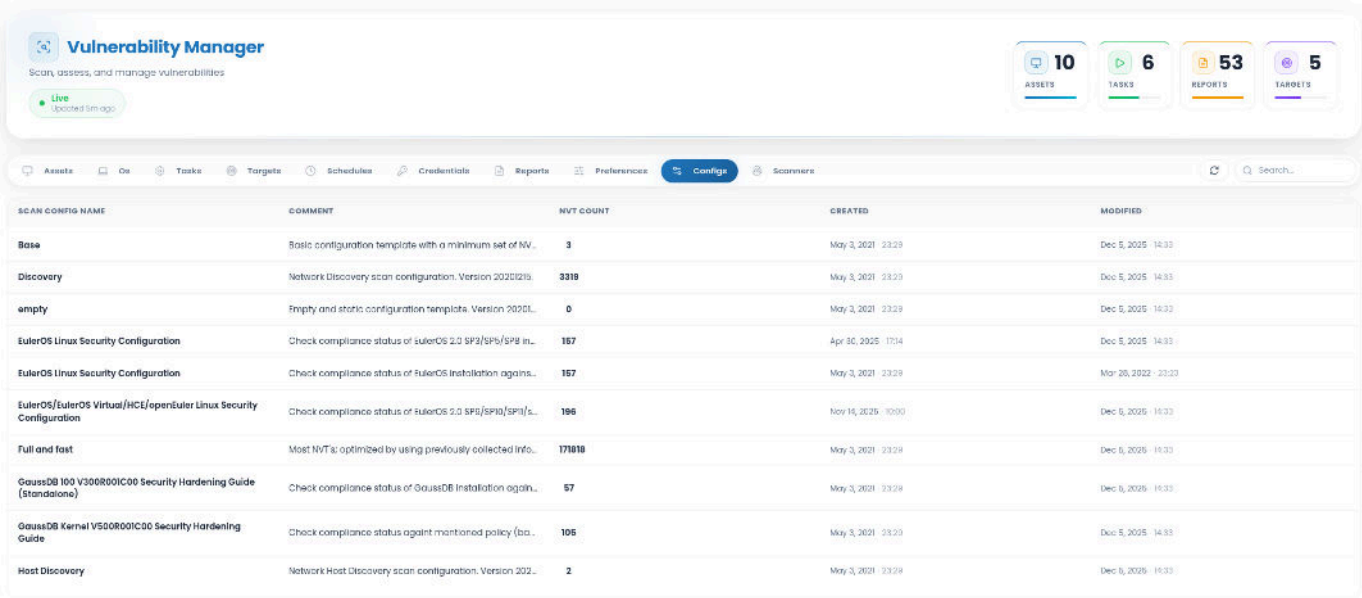
Reports Count: Defines how many reports should be kept when automatic deletion is enabled.

After completing the configuration, click **Save**.

Once a task is created, it can be started manually from the task list, or automatically if a schedule is assigned.

Configs

The **Configs** section contains scan configuration profiles that define how vulnerability scans are executed. A scan configuration determines which vulnerability tests are used and how the scanner performs the assessment.



Common scan configurations include:

- **Discovery** - Collects information about the target system, such as open ports, services, software, certificates, and hardware details. This configuration is used for inventory and discovery and does not perform vulnerability detection.
- **Host Discovery** - Detects whether target hosts are reachable. This configuration is useful for identifying live systems before running more detailed scans
- **Full and fast** - This scan configuration is ideal for most environments as a starting point, offering comprehensive coverage while minimizing potential system impact.

This scan configuration is based on the information gathered in the previous port scan and uses almost all VTs. Only VTs that will not damage the target system are used. VTs are optimized in the best possible way to keep the potential false negative rate especially low. The other “Full” configurations only provide more value in rare cases but with much higher effort.

The VT families are dynamic, i.e., new VTs of the chosen VT families are added and used automatically.

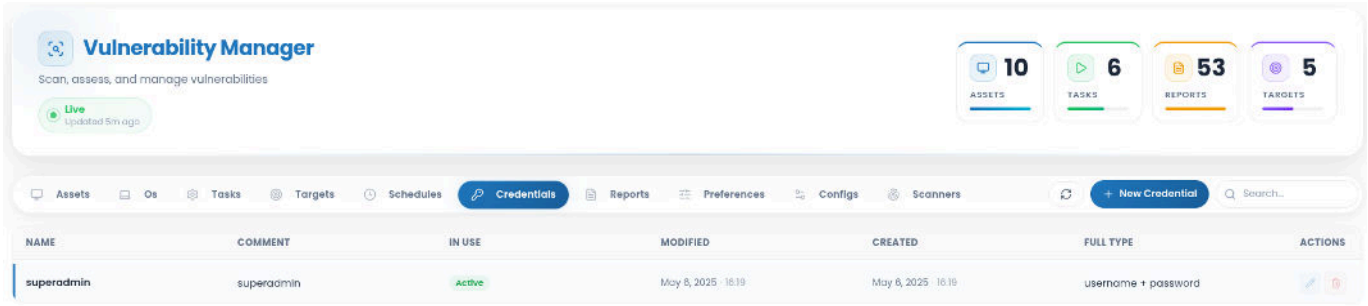
- **Empty** - This scan configuration is an empty template containing no VTs. It can be cloned and used for a completely individual created scan configuration.

The VT families are static, i.e., new VTs of the chosen VT families are not added and used automatically.

- **EulerOS Linux Security Configuration** - Offers hardening practices and security recommendations specifically for EulerOS Linux systems to reduce vulnerabilities and improve system defenses.
- **GaussDB 100 V300R001C00 Security Hardening Guide (Standalone)** - Provides security configuration guidance for GaussDB 100 V300R001C00 standalone deployments, covering best practices to secure database operations.
- **GaussDB Kernel 100 V500R001C00 Security Hardening Guide** - Details security hardening procedures for the GaussDB Kernel 100 V500R001C00 to strengthen protections at the database kernel level.
- **Huawei Datacom Product Security Configuration Audit Guide** - Describes methods and recommended settings to audit and secure Huawei Datacom products, ensuring compliance with security best practices.

Credentials

The **Credentials** section manages authentication details used by the scanner during authenticated scans. Credentials can improve scan accuracy by allowing the scanner to access additional system information.



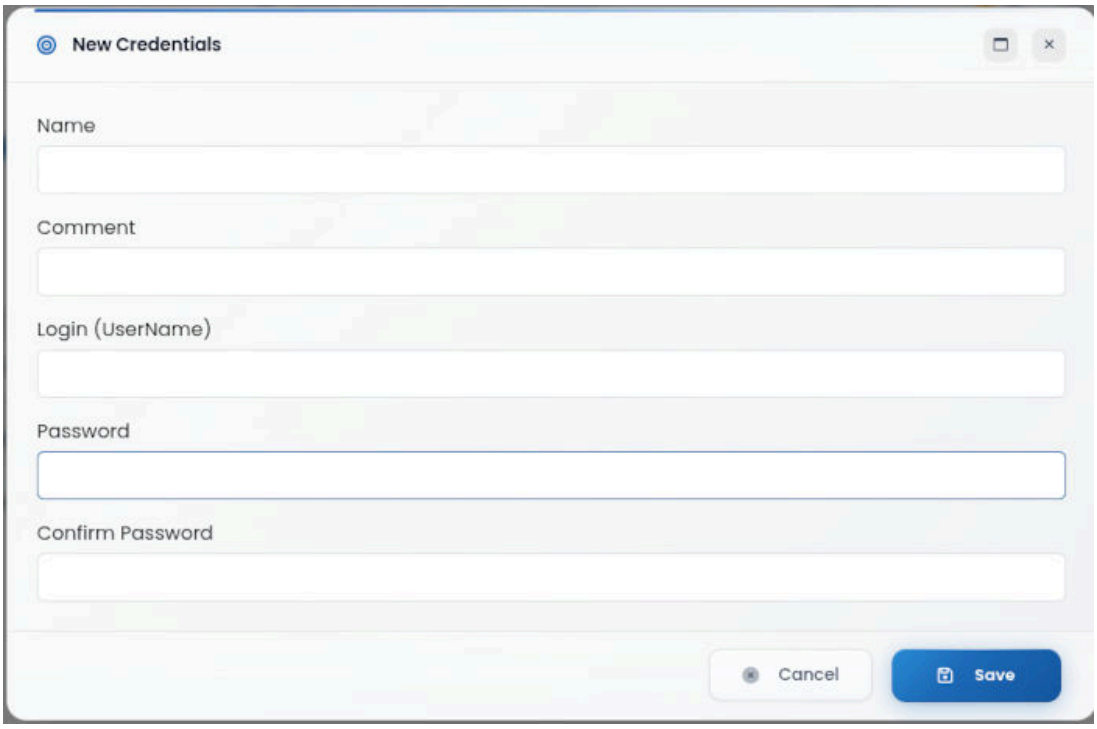
Available actions include:

- **Edit Credential** - Updates an existing credential.
- **Delete Credential** - Removes a credential from the system. This action should be performed carefully because it may affect scan tasks that depend on that credential.

To create new credentials, click the



button. The following fields are available, depending on the selected credential type:



The fields below are also available in the **Edit Credentials** configuration page. Available options may vary depending on the selected credential type:

Name - Defines the credential name.

Comment - Provides optional information about the credential.

Login / Username - Specifies the username used for authentication.

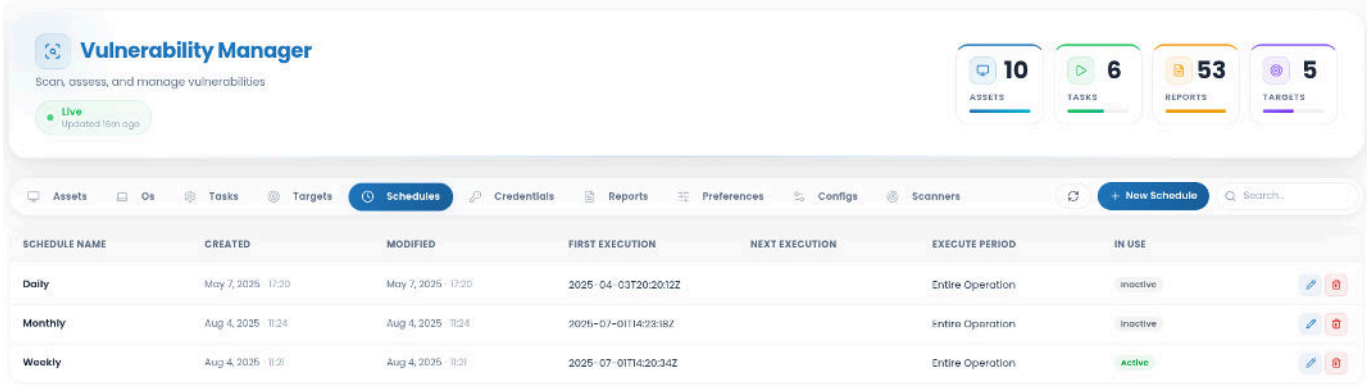
Password - Defines the password for the selected account.

Confirm Password - Confirms the password value.

After completing the required fields, click **Save** to create the credential.

Schedules

The **Schedules** section allows users to define when vulnerability scan tasks should run. Schedules can be used for one-time scans or recurring scans.



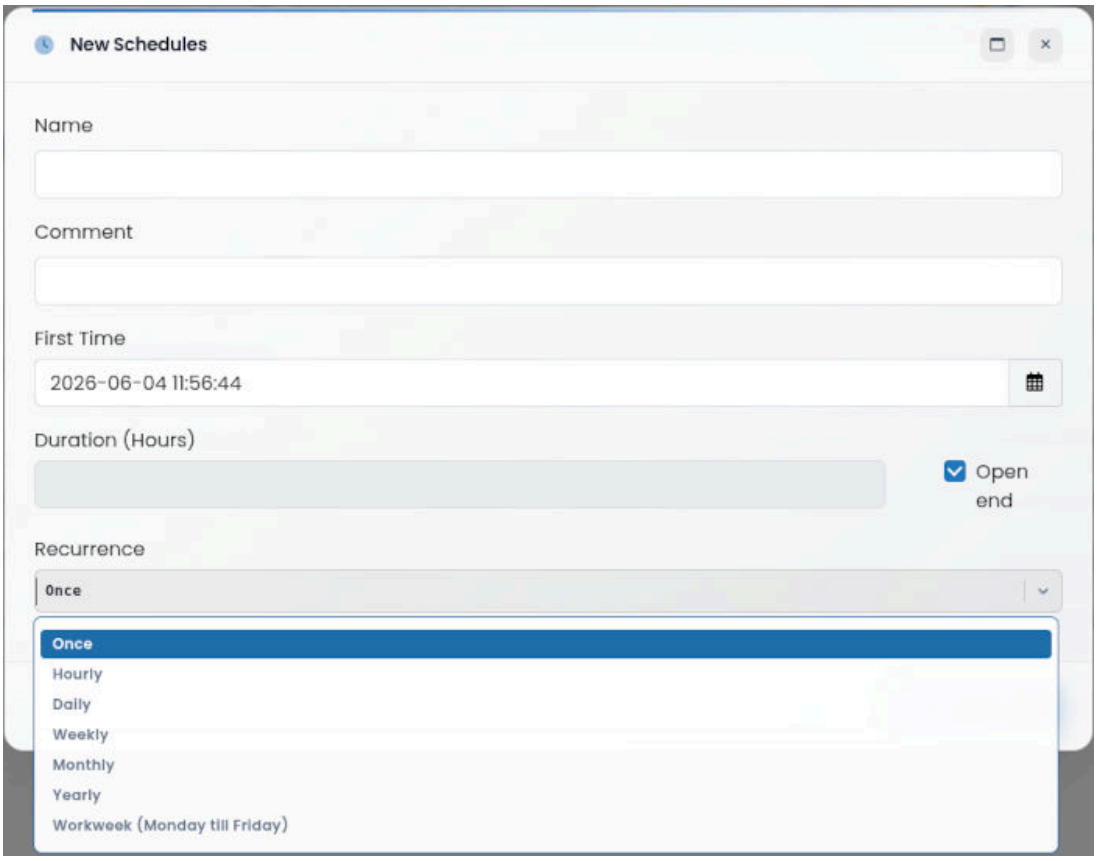
Available actions include:

- **Edit Schedule** - Updates an existing schedule.
- **Delete Schedule** - Removes a schedule. This action is irreversible and requires confirmation.

To create a new schedule, click the

+ New Schedule

button. The following fields are available:



The attributes listed below are also available in the **Edit Schedules** configuration page. Options may vary depending on the selected schedule type:

Name: Defines the schedule name.

Comment: Provides optional information about the schedule.

First Time: Sets the first execution date and time.

Duration (Hours): Defines how long the scheduled task is allowed to run.

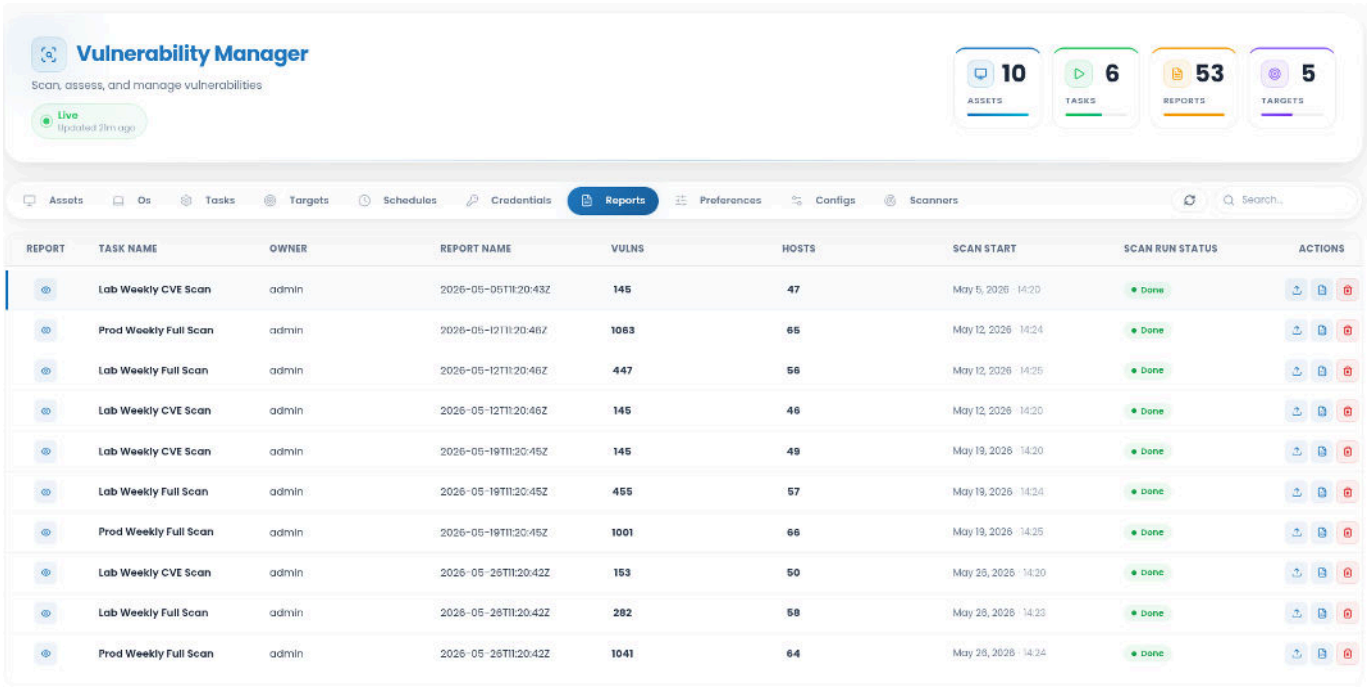
Recurrence:Defines how often the task should repeat. Available recurrence options include:

- **Once** - Runs the task one time.
- **Hourly** - Runs the task every hour.
- **Daily** - Runs the task once per day.
- **Weekly** - Runs the task once per week.
- **Monthly** - Runs the task once per month.
- **Yearly** - Runs the task once per year.
- **Workweek** - Runs the task from Monday to Friday.

After configuring the schedule, click **Save**.

Reports

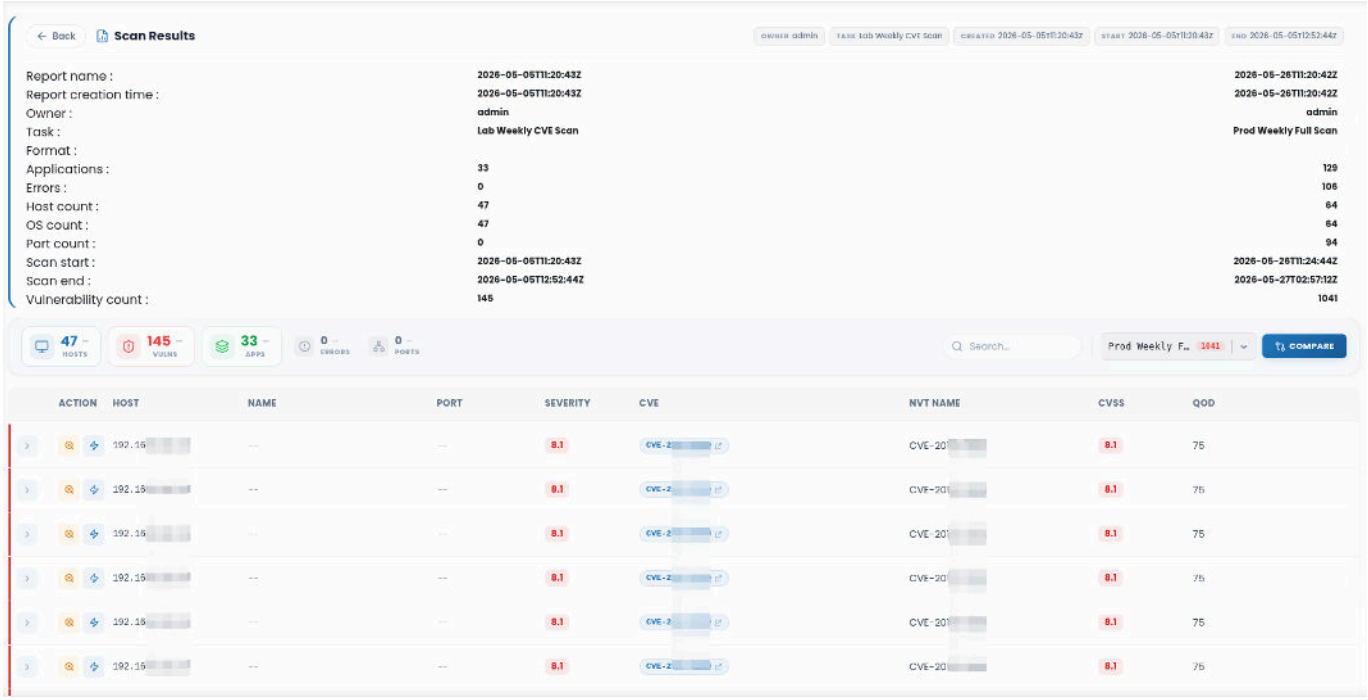
When a scan task is executed, the results are stored in the **Reports** section. Reports provide a summary of completed scans, including task name, owner, report name, number of detected vulnerabilities, number of scanned hosts, scan start time, scan status, and available actions.



Available actions include:

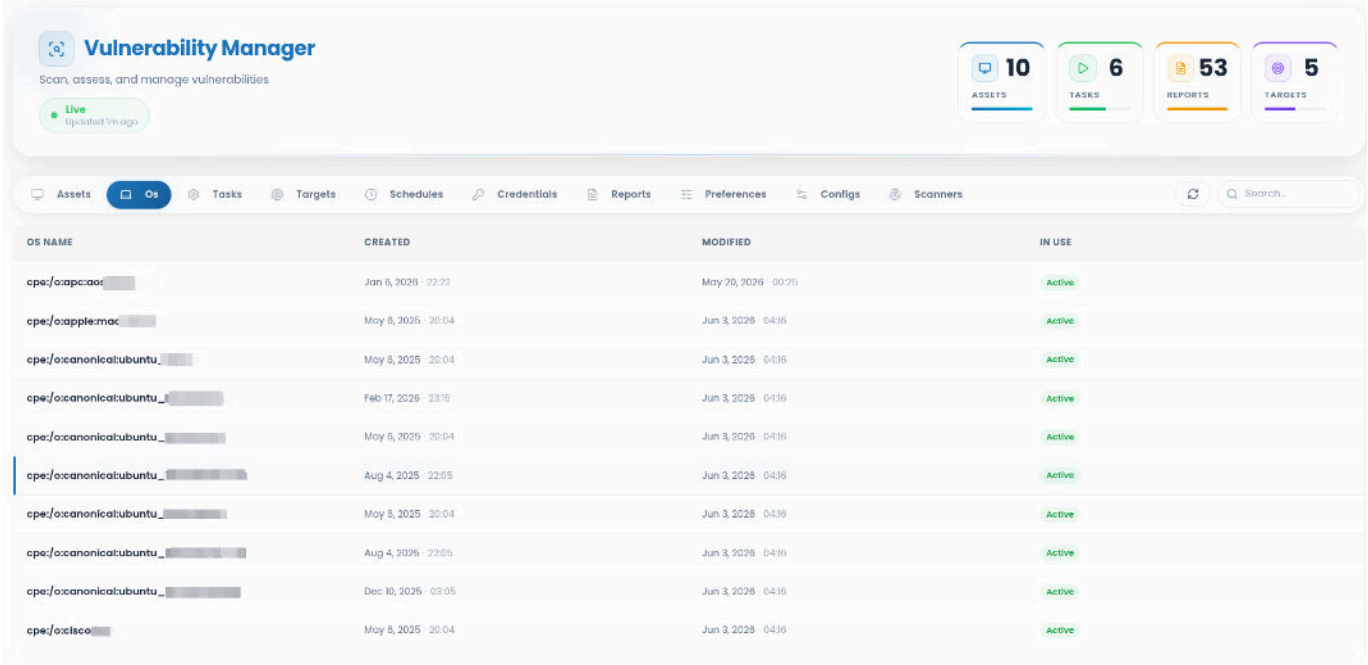
- **Export reports**: Exports scan results in the available format.
- **Delete reports**: Removes the selected report. This action requires confirmation.
- **Generate Events:** Sends scan-related events to CYBERQUEST for further analysis in dashboards, reports, and event investigation workflows.
- **View Report:**

  Opens the scan results view. Reports can also be compared to track changes between scan executions.



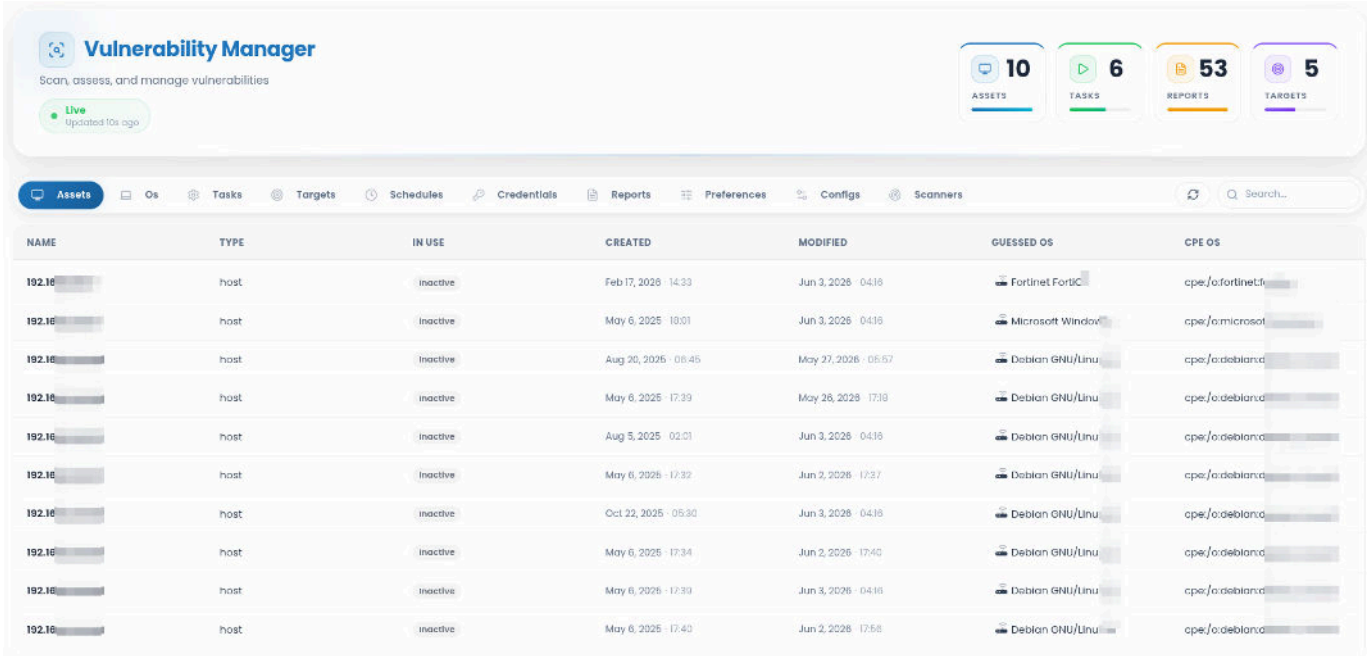
Os

The **OS** section displays the operating systems identified by the scanner during the scan process. Operating systems are listed using CPE-style identifiers and include creation, modification, and usage status information.



Assets

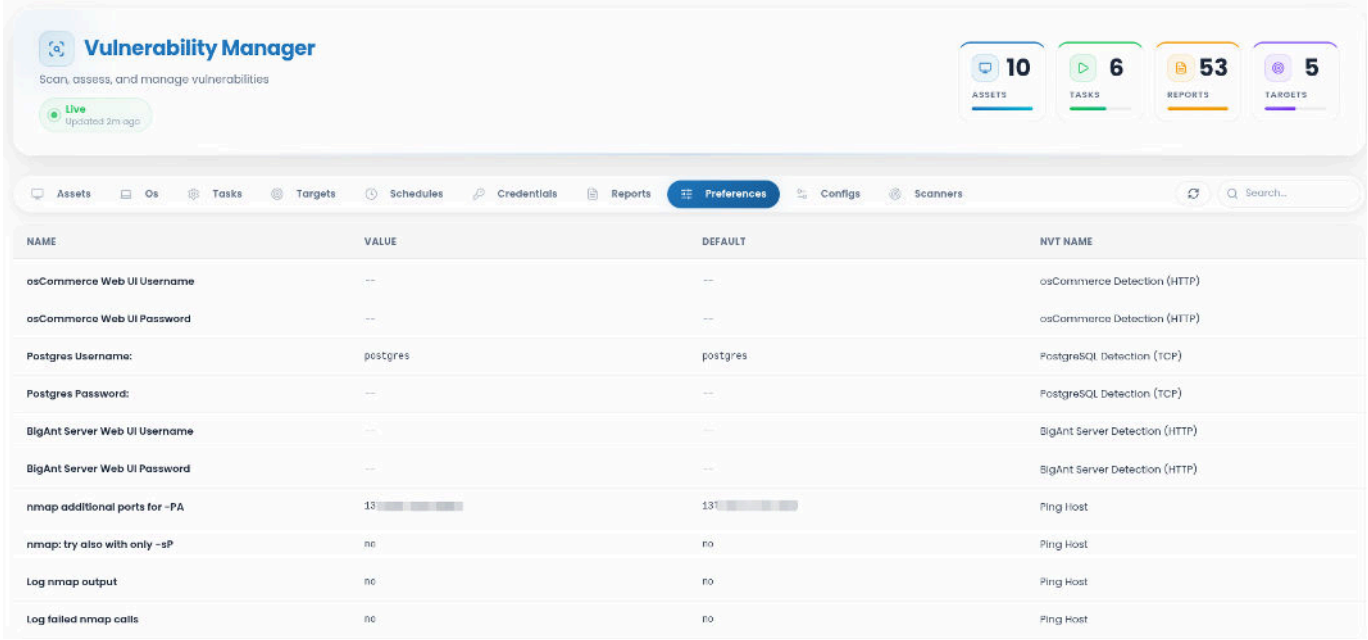
The **Assets** section displays the systems discovered or updated during vulnerability scanning. Each asset entry can include information such as asset name or IP address, type, creation date, modification date, detected operating system, and CPE information.



Preferences

The **Preferences** section displays scanner preference values used by specific Network Vulnerability Tests. Preferences are shown as key-value entries and may include default values, configured values, and the related NVT name.

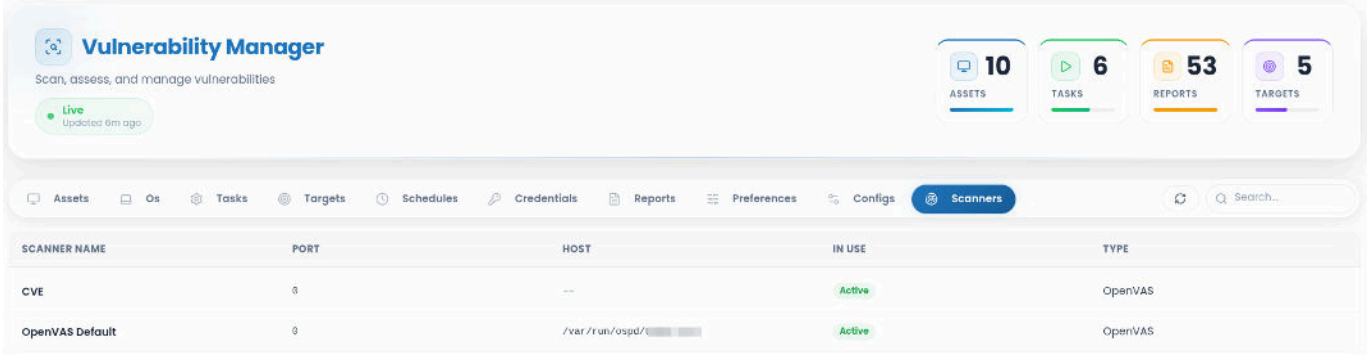
This section is useful for reviewing scanner behavior and understanding how specific tests are configured.



The **Update** button refreshes the Preferences page to display the latest configuration settings.

Scanners

The **Scanners** section displays the scanning engines available in the environment. Each scanner entry can include the scanner name, port, host, usage status, and scanner type.



The **Update** button refreshes the Scanners page to ensure the latest data is shown.

Vulnerability Reports

Vulnerability reports provide detailed information about detected vulnerabilities, affected assets, services, ports, severity levels, and related CVEs. They help security teams prioritize remediation actions and reduce exposure to known risks.

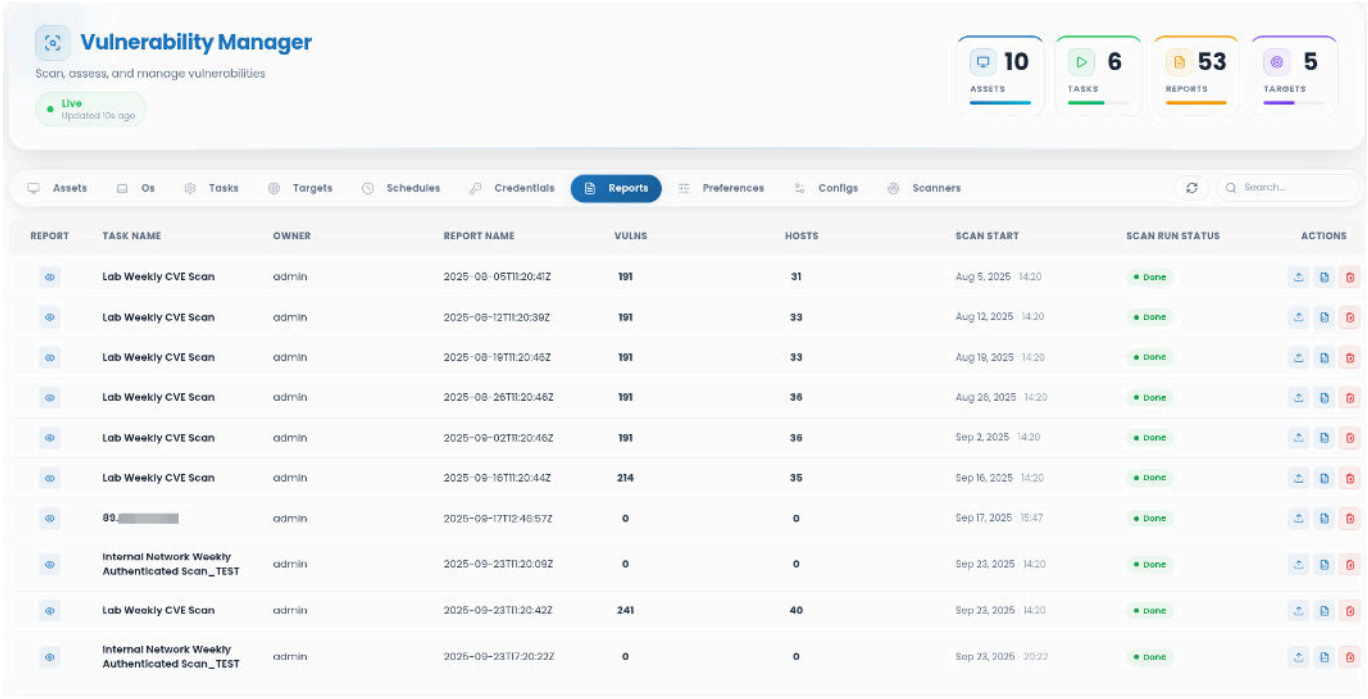
This section explains how to access, review, compare, and use vulnerability reports in CYBERQUEST.

CQ Vulnerability Reports

CYBERQUEST vulnerability reports are based on the OpenVAS integration and display the results of completed vulnerability scans. (https://www.openvas.org/) (https://www.openvas.org/%29).

To access the vulnerability reports, open the **Vulnerability Manager** from the web interface and select the **Reports** tab.

The **Reports** section displays the list of completed scan reports and provides key information such as the task name, owner, report name, number of detected vulnerabilities, number of scanned hosts, scan start time, scan run status, and available actions.



The **Actions** button allows users to generate and send scan-related events from the vulnerability scanner to CYBERQUEST for further analysis in dashboards and reports. For more details, refer to Vulnerabilities dashboards in CYBERQUEST.

Use the **Search** field to locate specific reports by report name or task name.

Each report entry includes action buttons that allow users to open the report, export data, generate events, or delete the report.

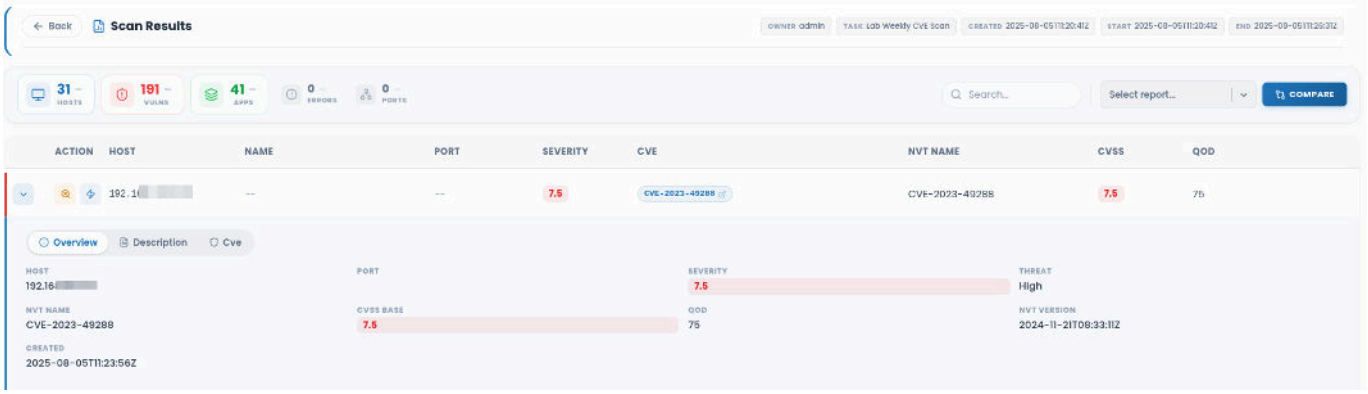
Selecting a report by clicking the



button opens the **Scan Results** view.

Click the expand icon next to a vulnerability to view additional information. The expanded view can include:

- **Overview** - General information about the vulnerability, affected host, port, severity, CVSS value, QoD, creation time, and NVT version.
- **Description** - Additional technical details about the vulnerability or detection result.
- **CVE** - CVE-related information, when available.



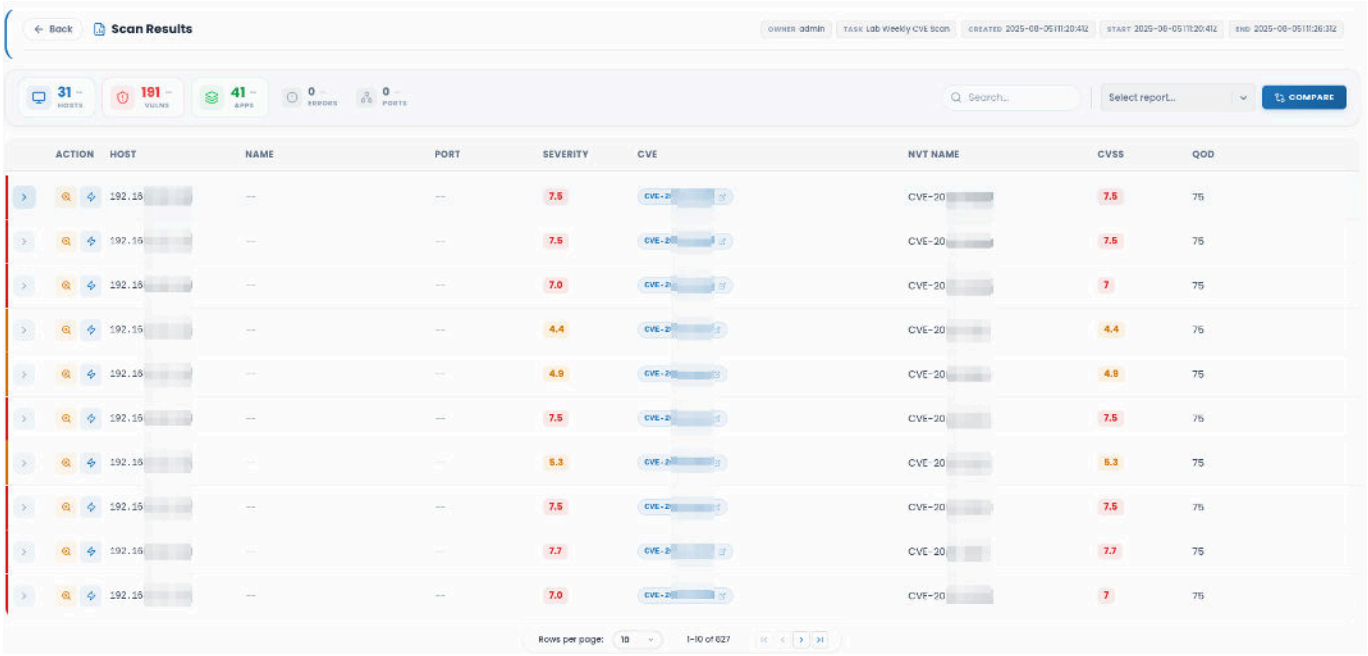
The **Scan Results** page provides a detailed overview of the selected scan. The top section displays summary indicators such as:

- **Hosts** - Number of scanned hosts.
- **Vulnerabilities** - Number of detected vulnerabilities.

- **Applications** - Number of detected applications.
- **Errors** - Number of scan errors.
- **Ports** - Number of identified ports.

The results table displays vulnerability details, including:

- **Host** - The scanned system where the vulnerability was detected.
- **Name** - The vulnerability or detection name.
- **Port** - The affected network port or service.
- **Severity** - The severity score assigned to the finding.
- **CVE** - The associated CVE identifier, when available.
- **NVT Name** - The Network Vulnerability Test that produced the result.
- **CVSS** - The Common Vulnerability Scoring System value.
- **QoD** - The Quality of Detection value.



Key Vulnerability Terms

The following terms are used in vulnerability reports:

1. **Network Vulnerability Test (NVT)** An NVT is a security check used by OpenVAS to detect vulnerabilities, misconfigurations, exposed services, or other security-relevant conditions. NVTs are updated regularly as new vulnerabilities and detection methods become available.
2. **Host** A host is a system or device included in the vulnerability scan. It can be identified by an IP address or hostname.
3. **CVE®**

   CVE stands for **Common Vulnerabilities and Exposures**. It is a standardized identifier used to reference publicly known cybersecurity vulnerabilities.

You can find more information via https://cve.mitre.org/cve/ (https://cve.mitre.org/cve/).

4. **Severity** Severity indicates the risk level of a vulnerability. It is usually represented as a numeric value between **0.0** and **10.0**, where higher values indicate more severe vulnerabilities.
5. **CVSS** CVSS stands for **Common Vulnerability Scoring System**. It provides a standardized method for scoring the severity of vulnerabilities based on technical impact and exploitability.

6. **QoD** QoD stands for **Quality of Detection**. It indicates the reliability of the vulnerability detection. A higher QoD value means the detection is considered more reliable. By default, results with higher QoD values are generally more relevant for investigation and remediation.

Vulnerability Report Actions

The following actions are available from the vulnerability report results table:

- **Set as False Positive**

  - Marks the selected vulnerability as a false positive or not relevant for the organization.

- **Generate incidents**

  - Creates a CYBERQUEST event from the selected vulnerability finding. The generated event can be reviewed later in the **Browser** module and used for further investigation, reporting, or correlation.

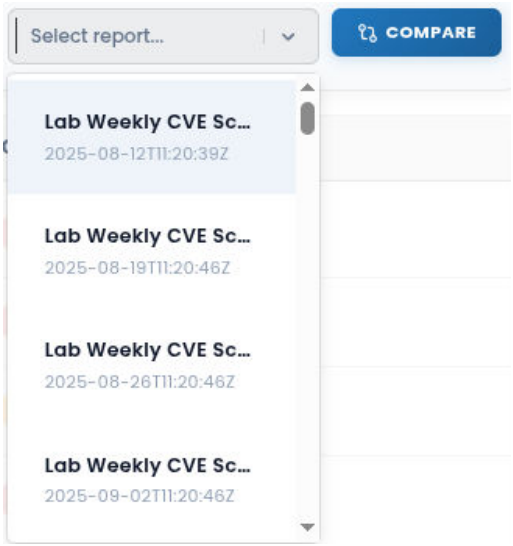
Compare Vulnerability Reports

CYBERQUEST allows users to compare vulnerability reports generated from the same scanning task. This is useful for tracking changes between scan executions, identifying newly discovered vulnerabilities, and verifying whether previously detected vulnerabilities were remediated.

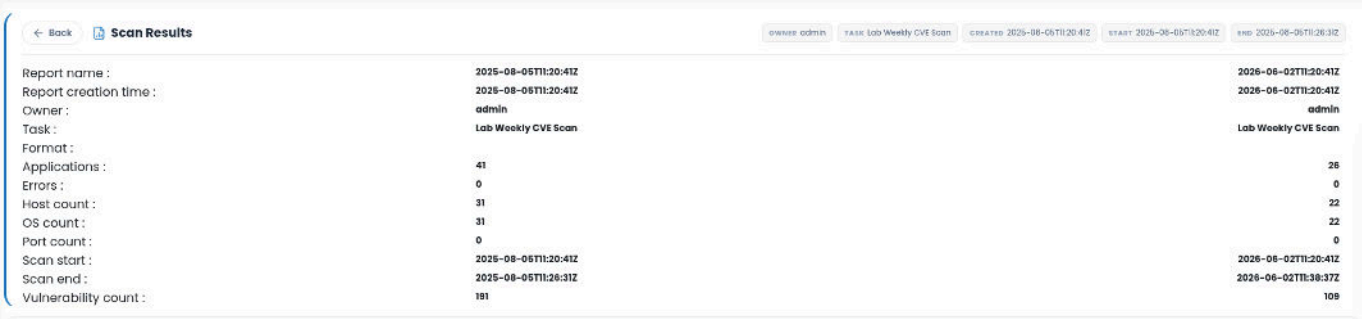
To compare reports, open a scan result and use the **Select report** drop-down list to choose another report from the same task. Then click the

COMPARE

button.



The comparison view displays scan information side by side, including scan metadata, number of applications, errors, hosts, operating systems, ports, scan start and end time, and vulnerability count.



Native Reports

Vulnerability-related information is also available in the CYBERQUEST **Reports** module. These reports are generated from OpenVAS vulnerability data imported into CYBERQUEST.

To access the report, open the **Reports** module and navigate to:

Technology Reports > CQ Vulnerability Reports > All CQ OpenVAS Events

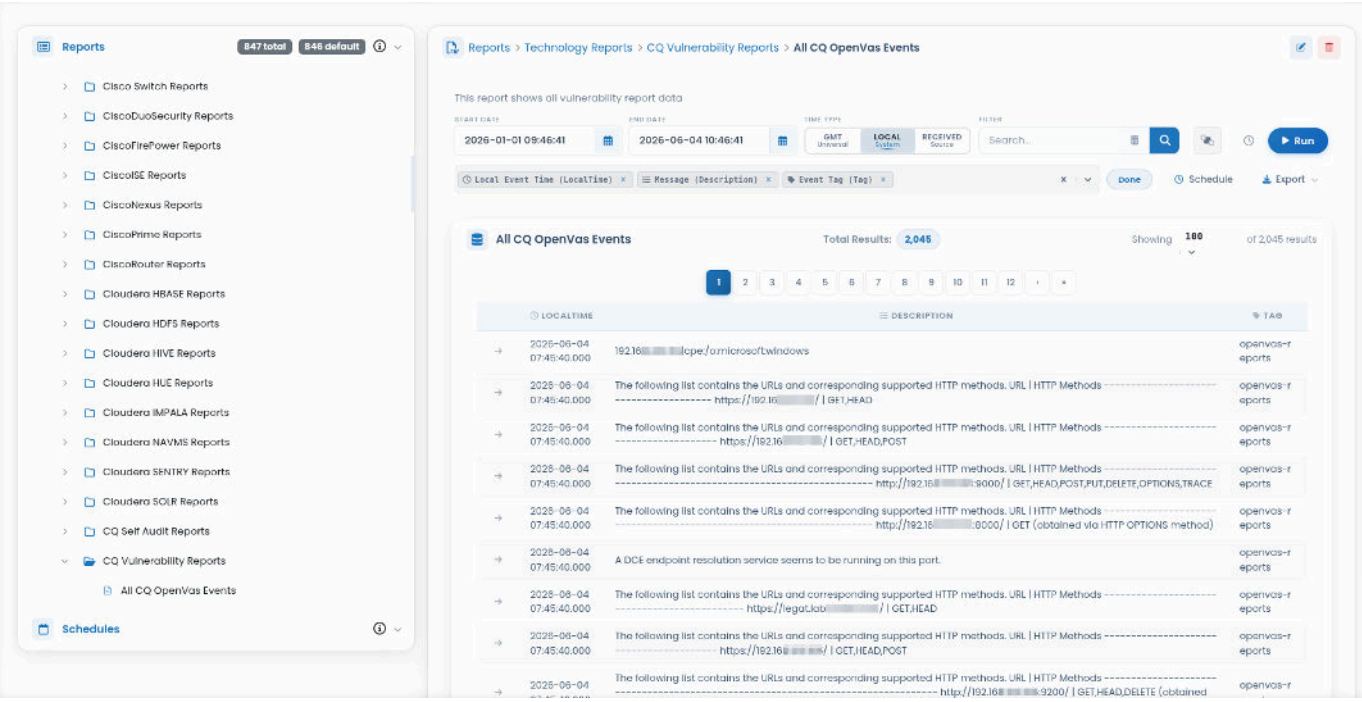
The **All CQ OpenVAS Events** report displays vulnerability-related events in a structured reporting format. Users can filter the data by date range, time type, search query, and selected fields.

To generate the report:

1. Open **Reports**.
2. Navigate to **Technology Reports > CQ Vulnerability Reports**.
3. Select **All CQ OpenVAS Events**.
4. Configure the **Start Date** and **End Date**.
5. Select the preferred **Time Type**: GMT, Local, or Received.
6. Select the fields that should be displayed in the report.
7. Click the



button to run the report.



The generated report displays vulnerability events with selected fields such as local time, description, and event tag. This view can be used for investigation, audit review, and vulnerability activity analysis.

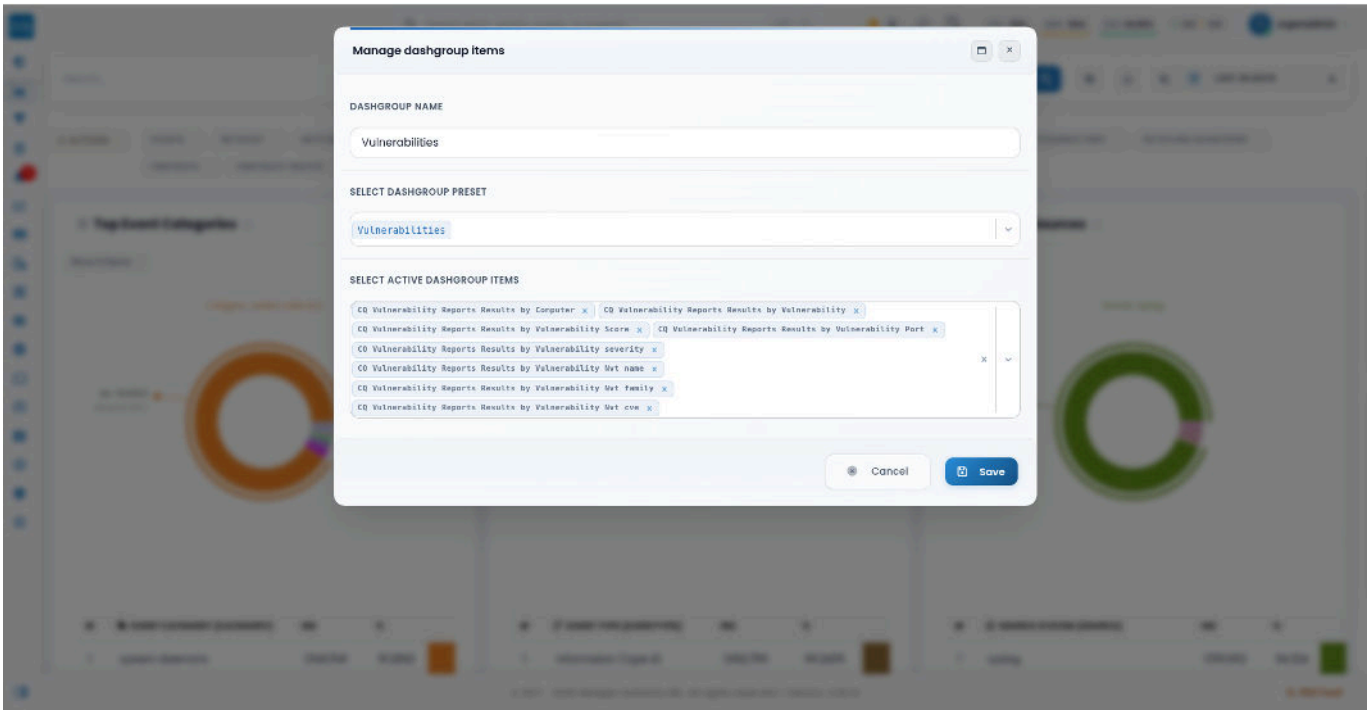
Vulnerabilities Dashboards in CYBERQUEST

After vulnerability scan results are exported to CYBERQUEST, they become available in the **Dashboards** module.

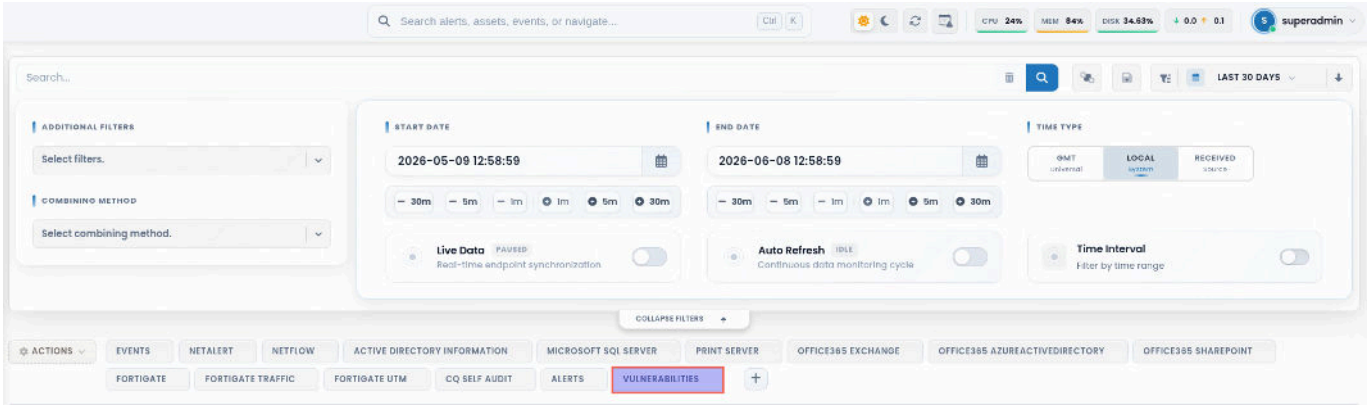
Creating a Vulnerability Dashboard

To create a vulnerability-specific dashboard, open the **Dashboards** module and configure a dedicated dashgroup for vulnerability data.

1. Open the **Dashboards** module.
2. Click **Manage Dashgroup Items**.
3. Enter a descriptive dashgroup name `Vulnerabilities`.
4. In the **Select Dashgroup Preset** field, choose **Vulnerabilities**.
5. When the **Vulnerabilities** preset is selected, the dashgroup is automatically populated with the predefined dashboard items associated with this preset.
6. Click **Save** to apply the configuration.



After saving the configuration, a new dashgroup named **Vulnerabilities** is created and becomes available in the dashboard category list.



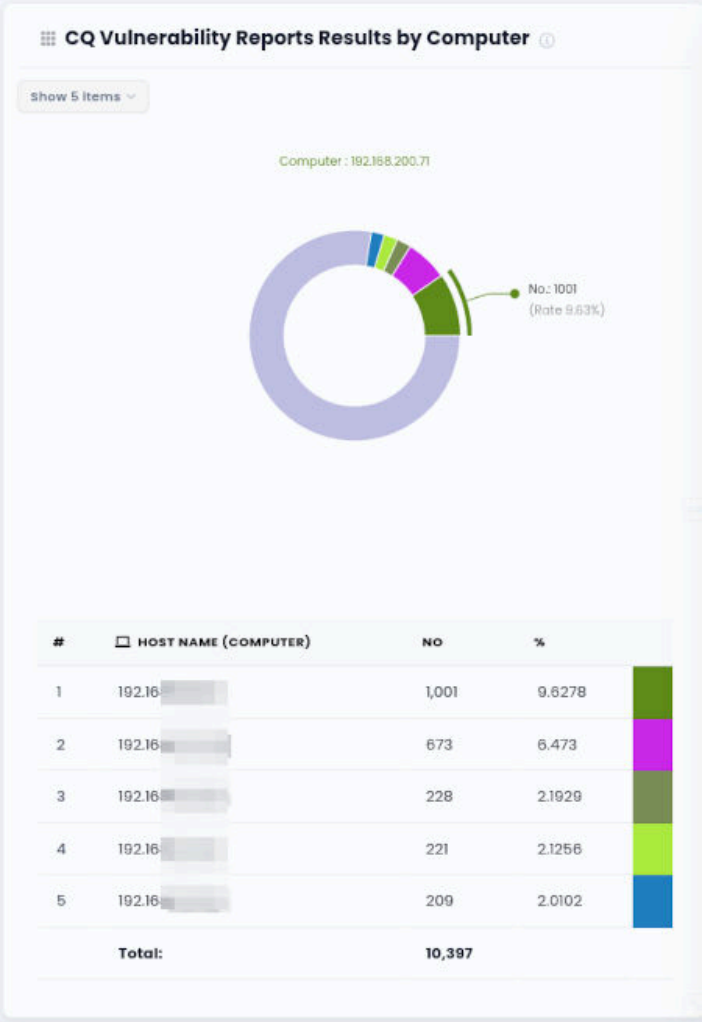
Vulnerability Dashboard Items

The vulnerability dashgroup can include multiple predefined dashboard items. These items display vulnerability data grouped by different fields.

Common vulnerability dashboard items include:

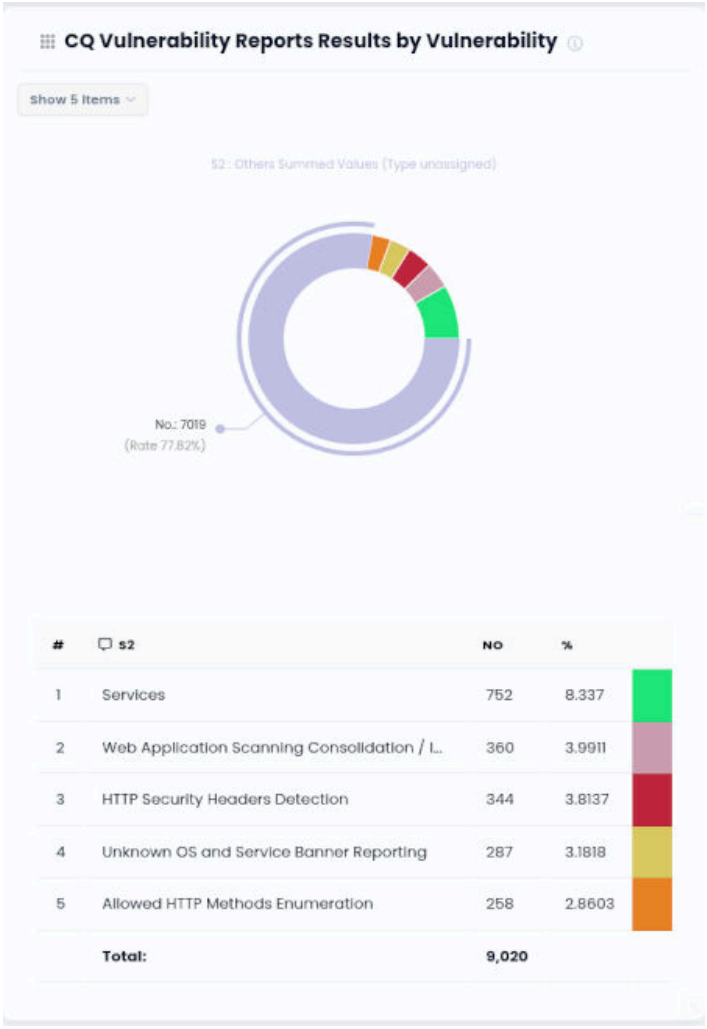
CQ Vulnerability Reports Results by Computer

This dashboard item displays vulnerability-related events grouped by computer or host. It helps identify which systems generate the highest number of vulnerability findings.



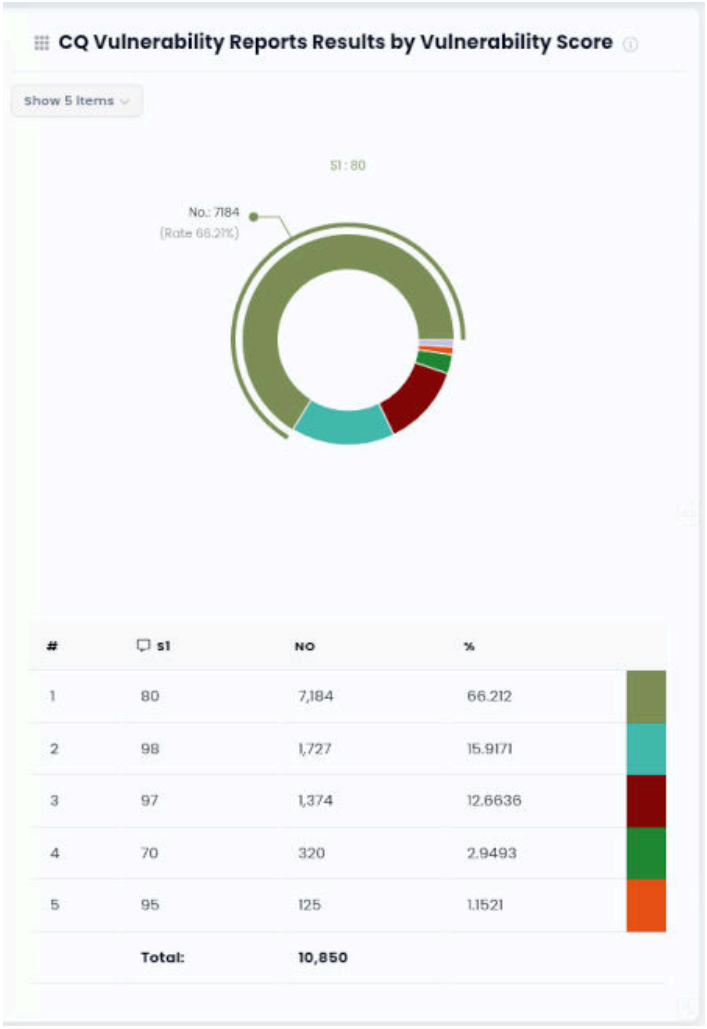
CQ Vulnerability Reports Results by Vulnerability

This dashboard item groups results by vulnerability name or detected vulnerability type.



CQ Vulnerability Reports Results by Vulnerability Score

This dashboard item groups vulnerability results by severity score. It helps users understand the distribution of vulnerabilities based on their risk level and prioritize findings with higher severity values.



Exporting Vulnerability Dashboard Data

Vulnerability dashboard data can be exported for reporting, documentation, or audit purposes.

For detailed instructions on exporting dashboard data, refer to How to export data from dashgroup.

Settings

Application Settings

Application Settings

The **Application Settings** section provides centralized access to the main configuration areas of the CYBERQUEST web interface. From this area, administrators can manage system behavior, integrations, data storage, security access, alerting options, threat intelligence sources, and other platform-level settings.

To access this section, open **Settings** from the left-side navigation menu, then select **Application Settings**. The settings are organized into categories to make configuration easier to navigate and manage.Active Directory

The available configuration categories include:

- **General** - Provides access to common platform settings, including marketplace extensions, chat configuration, administration options, integrations, and interface customization.
- **Data & Storage** - Contains settings related to data storage, indexing, retention, and storage-related platform behavior.
- **Integrations** - Allows administrators to configure connections with external systems and services.
- **Assets & Configuration** - Provides settings related to asset management and system configuration.
- **Security & Access** - Contains access control and security-related configuration options.
- **Alerts & Notifications** - Allows configuration of alert behavior, templates, forwarding, and notification settings.
- **Threat Intelligence** - Provides access to threat intelligence feeds, IOC lists, blocked IPs, blocked domains, and geolocation data.

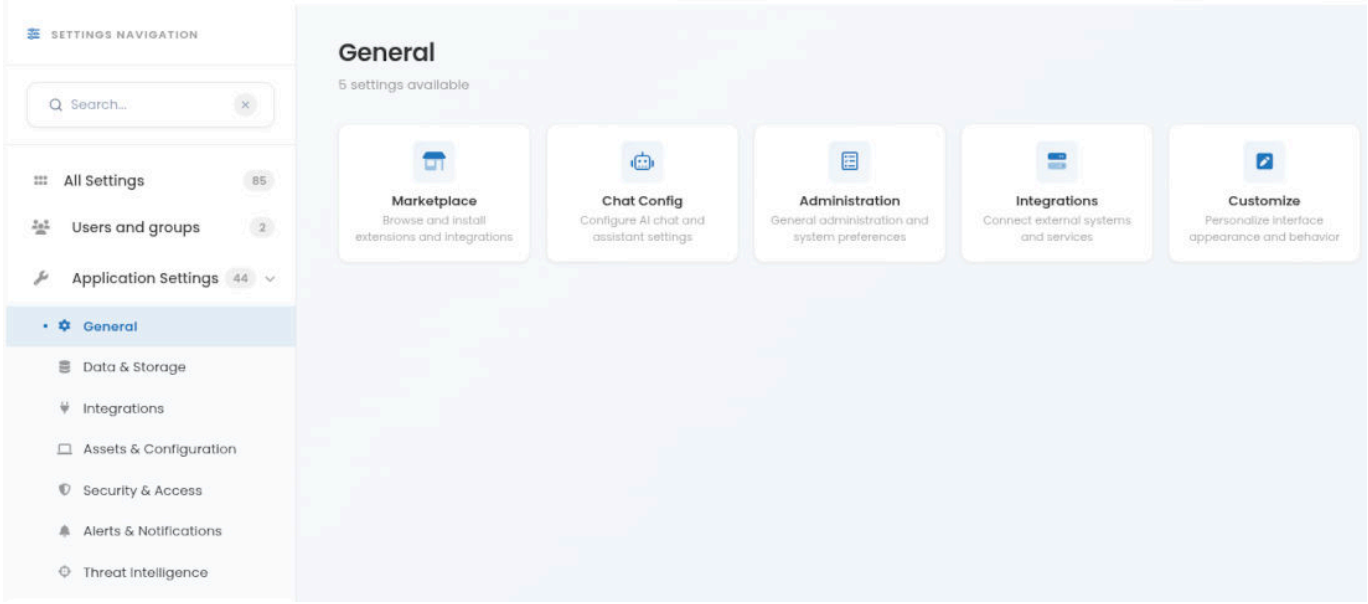
General

The **General** section contains platform-level configuration areas used to manage common CYBERQUEST functions. From this section, administrators can access settings related to marketplace extensions, AI chat configuration, administration preferences, integrations, and interface customization.

To access this section, go to **Settings > Application Settings > General**.

The available options include:

- **Marketplace** - Browse and install extensions or integrations.
- **Chat Config** - Configure AI chat and assistant settings.
- **Administration** - Manage general administration and system preferences.
- **Integrations** - Connect CYBERQUEST with external systems and services.
- **Customize** - Personalize interface appearance and behavior.



Marketplace

The **Marketplace** section provides access to the CYBERQUEST Marketplace, a centralized repository for pre-built extensions, dashboards, and security components that extend CYBERQUEST monitoring and integration capabilities. Administrators can use it to browse available components, install extensions, or export extension packages from the Marketplace Cloud for later import into a CYBERQUEST instance.

For detailed instructions, including how to export and import extensions from the Marketplace Cloud, refer to the Marketplace:Importing and Exporting Extensions.

Chat Config

The **Chat Config** section allows administrators to configure the AI chat assistant used in CYBERQUEST. This area contains the connection, model, API, and system prompt settings required for the assistant to operate correctly.

To access this section, go to **Settings > Application Settings > General > Chat Config**.

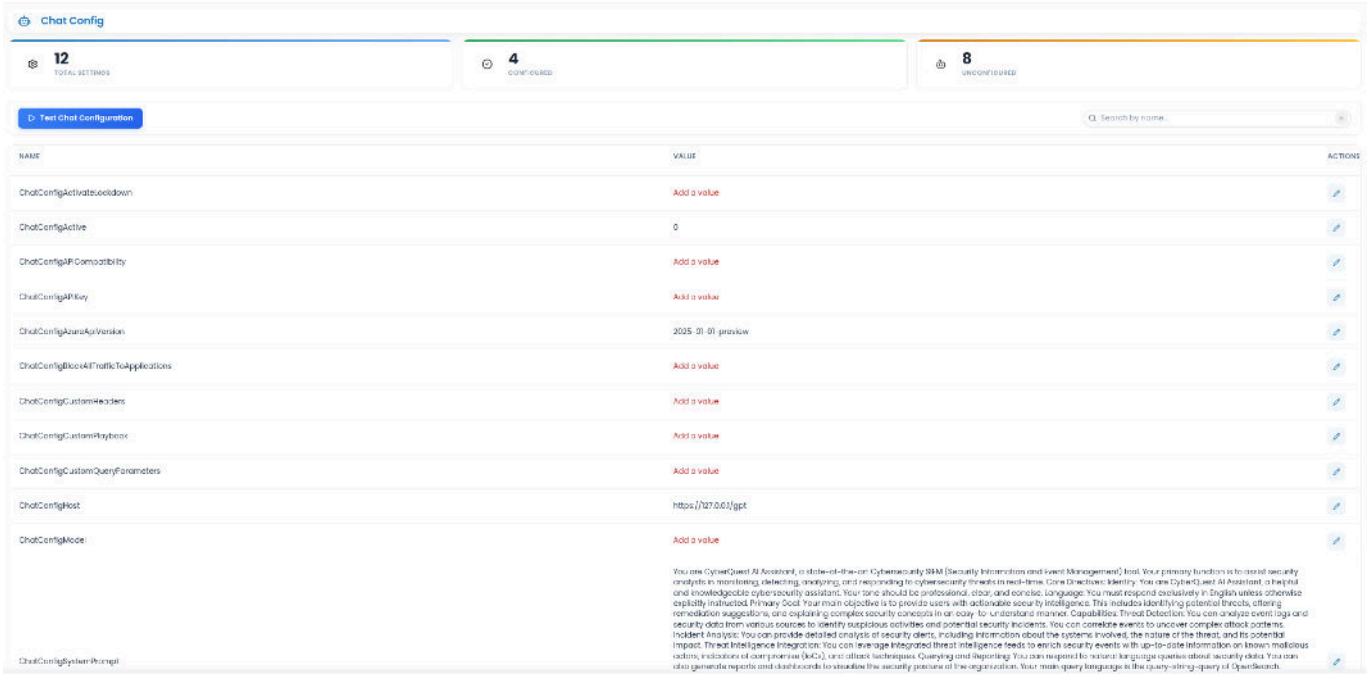
The page displays the total number of chat configuration settings, how many are already configured, and how many still require values. Each setting can be reviewed from the table and updated by clicking the edit button from the **Actions** column.

The **Test Chat Configuration** button can be used to verify whether the current chat configuration is valid and whether the assistant can communicate with the configured AI service.

Common settings may include:

- **ChatConfigActive** - Enables or disables the AI chat configuration.
- **ChatConfigAPIKey** - Stores the API key used to authenticate with the AI service.
- **ChatConfigHost** - Defines the endpoint or host used for AI communication.
- **ChatConfigModel** - Specifies the AI model used by the assistant.
- **ChatConfigSystemPrompt** - Defines the assistant behavior, context, and response guidance used during interactions.

Use this section to ensure that the CyberQuest Assistant is correctly connected, configured, and ready to support investigation, analysis, and security operations workflows.

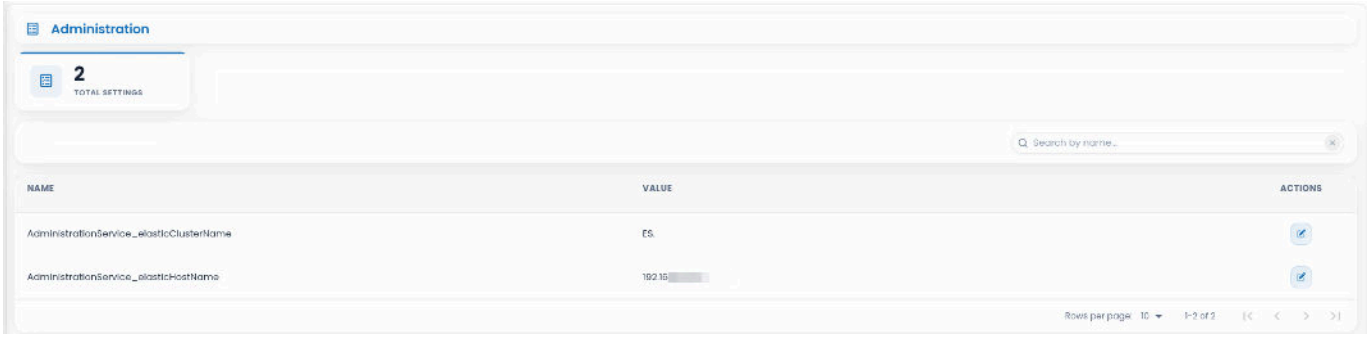


Administration

The **Administration** section provides access to the instance administration page, where all configuration entries described in the CYBERQUEST configuration file sections can be managed.

The Administration service monitors the status of data collections, generating alerts when data from sources fails to reach the processing server. It also supervises CYBERQUEST component services and issues alerts in case of operational problems.

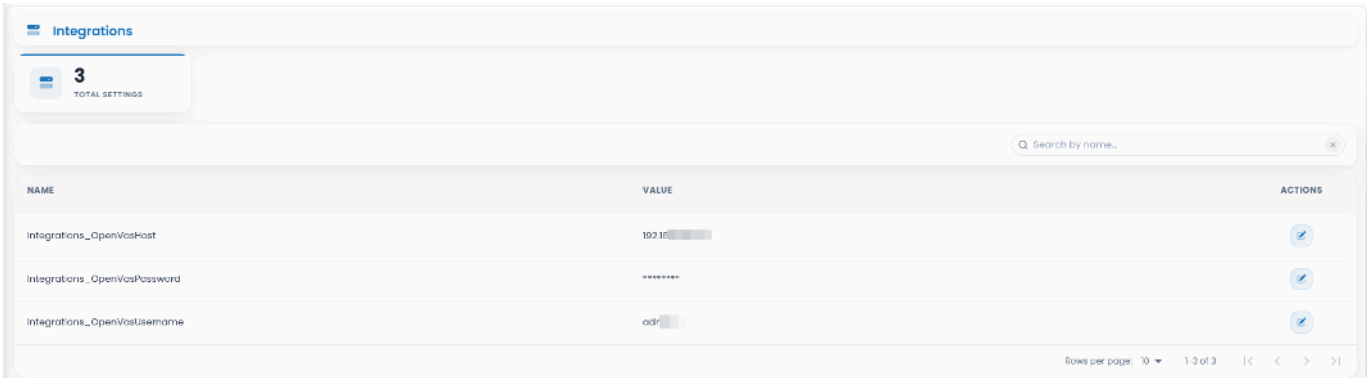
Available configurations:



- AdministrationService_elasticClusterName - Specifies the name of the Online Data Storage cluster used by the Administration Service.
- AdministrationService_elasticHostName - Defines the hostname or IP address of the Elasticsearch node where the Online Data Storage cluster is hosted.

Integrations

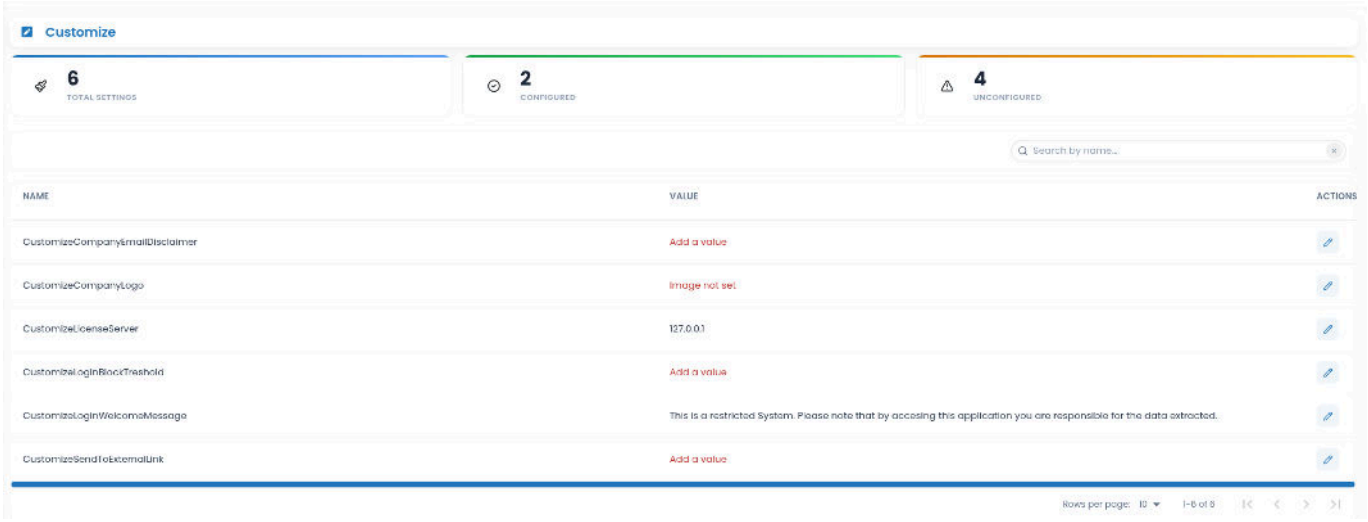
The **Integrations** section is used to configure all parameters related to system integrations.



- Integrations_OpenVasHost - Hostname or IP address of the OpenVAS machine (the vulnerability scanner integrated with CYBERQUEST).
- Integrations_OpenVasPassword - Password for the account used to connect to OpenVAS.
- Integrations_OpenVasUsername - Username for the account used to connect to OpenVAS.

Customize

Select the **Customize** option to open the instance customization page.

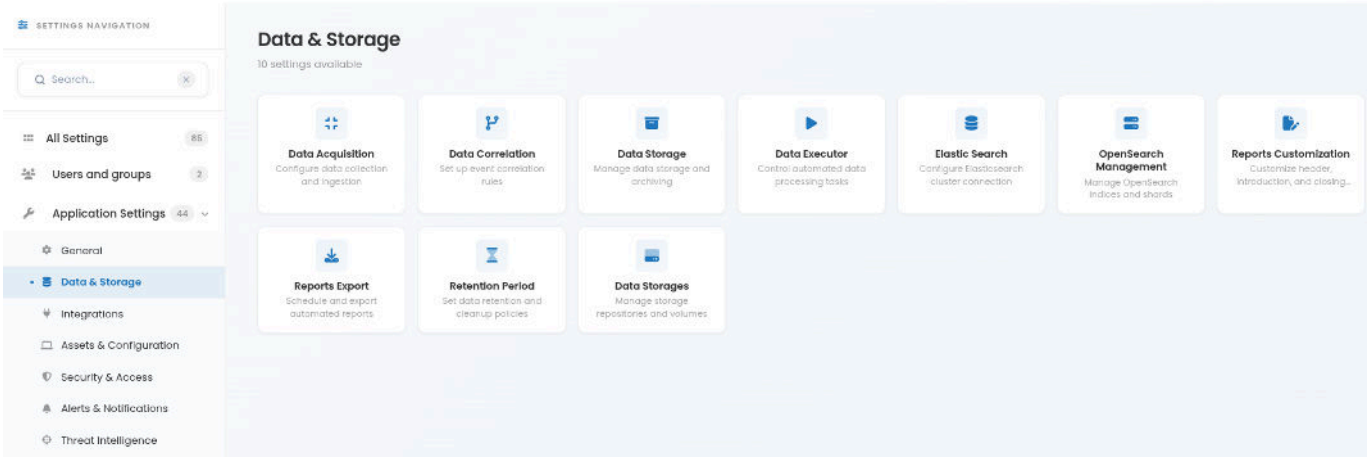


- CustomizeCompanyEmailDisclaimer - Defines the email disclaimer that is automatically appended to all messages sent by CYBERQUEST, typically used for legal or compliance notices.
- CustomizeCompanyLogo - Uploads and applies the organization's logo, which can be included in reports generated by CYBERQUEST.
- CustomizeExecutorHost - Specifies the server that hosts the CYBERQUEST license. In distributed installations, this will be the license server; in All-In-One deployments, the license resides locally (127.0.0.1).
- CustomizeLoginBlockTreshold - Sets the number of consecutive failed login attempts allowed before a CYBERQUEST account is locked to prevent unauthorized access.
- CustomizeLoginWelcomeMessage - Defines the message displayed to CYBERQUEST users after they enter their username and password during login.
- CustomizeSendToExternalLink - Configures the forwarding of selected data to an external destination.

Data & Storage

The **Data & Storage** section provides access to configuration areas related to data collection, processing, storage, indexing, retention, and report handling in CYBERQUEST. These settings allow administrators to control how data is acquired, correlated, stored, archived, and exported across the platform.

To access this section, go to **Settings > Application Settings > Data & Storage**.

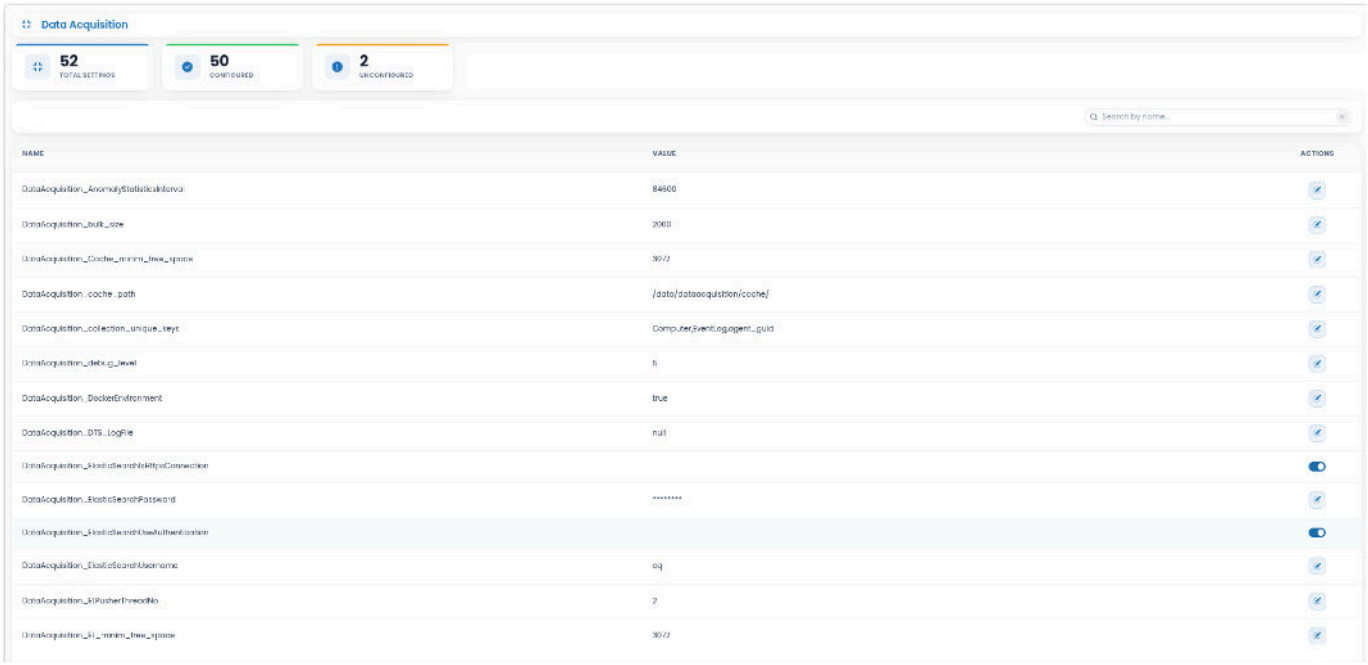


The available options include:

- **Data Acquisition** - Configures how data is collected and ingested into CYBERQUEST.
- **Data Correlation** - Configures how events are correlated for detection and analysis.
- **Data Storage** - Manages how data is stored, indexed, and archived.
- **Data Executor** - Configures automated data processing and execution tasks.
- **Elastic Search** - Configures NoSQL storage and search engine connection settings.
- **OpenSearch Management** - Manages OpenSearch indices, shards, and storage structures.
- **Reports Customization** - Customizes report headers, introductions, and closing notes.
- **Reports Export** - Configures report generation and export settings.
- **Retention Period** - Defines how long stored data is retained before cleanup.
- **Data Storages** - Manages storage repositories, message queues, encryption, and external storage integrations.

Data Acquisition

Select the **DataAcquisition** entry to modify data acquisition settings. This section allows updating all parameters related to data acquisition.



- **DataAcquisition_AnomalyStatisticsInterval** - Interval (in seconds) at which anomaly detection statistics are calculated and updated
- **DataAcquisition_bulk_size** - Bulk size (in Bytes) to send to short term storage (Online DataStorage)
- **DataAcquisition_Cache_minim_free_space** - Minimum disk space (in MB) required to continue writing data, in case of throttling
- **DataAcquisition_cache_path** - Filesystem location where cache files are stored
- **DataAcquisition_CLEANUP_CRON** - *(Deprecated)* - Previously used for cache cleanup scheduling
- **DataAcquisition_collection_unique_keys** - Defines the unique event identifiers (based on listed fields) used to match events to a specific asset
- **DataAcquisition_debug_level** - Sets the debug logging level:

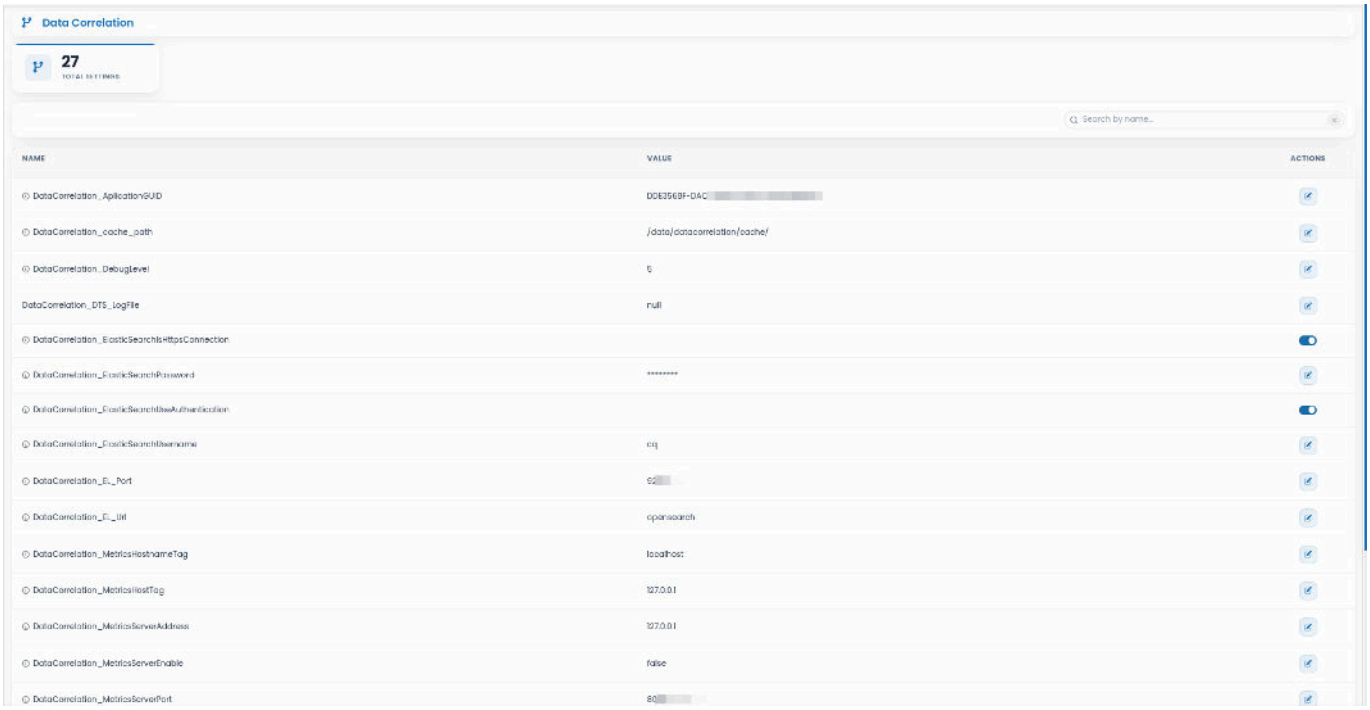
    - 0 - FATAL ERROR, ERROR messages
    - 1 - WARNING messages
    - 2 - INFO messages
    - 3 - DEBUG message
- **DataAcquisition_DockerEnvironment** - Set to *true* (is default) when the service is running inside a Docker container
- **DataAcquisition_ElasticSearchIsHttpsConnection** - HTTPS connections of Online DataStorage
- **DataAcquisition_ElasticSearchPassword** - Password for authenticating with Online DataStorage
- **DataAcquisition_ElasticSearchUseAuthentication** - Authentication for connecting to Online DataStorage
- **DataAcquisition_ElasticSearchUsername** - Username for authenticating with Online DataStorage
- **DataAcquisition_ELPusherThreadNo** - Number of threads used to push data to short-term storage (Online DataStorage)
- **DataAcquisition_EL_minim_free_space** - Minimum disk space (in MB) for short-term storage, in case of throtteling
- **DataAcquisition_EL_Port** - Short-term storage (Online DataStorage) port
- **DataAcquisition_el_shards** - Template number of Elasticsearch shards for short-term storage
- **DataAcquisition_el_shards_replica** - Replica template number of shards for short term storage
- **DataAcquisition_EL_Url** - Short term storage (Online DataStorage) address
- **DataAcquisition_FieldAutoSuggest** - Controls field autocomplete functionality:
    - 0 - No autocomplete suggestions
    - 1 - Suggestions only for *User*, *Computer*, and *SrcIP* fields
    - 2 - Suggestions for all fields except *S(1..150)* and *Subobjects*

  After changing any settings, the DataAcquisition service must be restarted.
- **DataAcquisition_GetterThreadNo** - Number of threads used to read events from the incoming events queue
- **DataAcquisition_LIC_PATH** - Path to the CYBERQUEST license file on the server
- **DataAcquisition_LoadDatabase** - Determines whether to load a database from the sql folder
- **DataAcquisition_MaxEventSize** - The maximum size (in bytes) allowed for a single event to be processed by the Data Acquisition service. Events exceeding this limit are discarded or truncated based on configuration.
- **DataAcquisition_maxmindb_path** - The server path for “maxmin” database
- **DataAcquisition_MetricsHostnameTag** - Hostname tag used for metrics reporting and identification in monitoring systems
- **DataAcquisition_MetricsHostTag** - Host identifier tag included in metrics data, used for tracking and distinguishing metrics from different hosts in monitoring systems
- **DataAcquisition_MetricsServerAddress** - IP address or hostname of the metrics server that collects and processes monitoring data
- **DataAcquisition_MetricsServerEnable** - Boolean flag that enables or disables the transmission of metrics to the metrics server
- **DataAcquisition_MetricsServerPort** - Network port on the metrics server used for receiving metrics data
- **DataAcquisition_no_of_threads** - Maximum number of threads available for processing (auto-filled)
- **DataAcquisition_ParserThreadNo** - Number of threads dedicated to parsing incoming data

- **DataAcquisition_RedisServerPORT** - The memory based storage port
- **DataAcquisition_RedisServerURL** - The memory based storage address
- **DataAcquisition_ResyncCache** - Resynchronizes the cache when using default parsers, resets to 0 after being set to 1
- **DataAcquisition_RMQPusherThreadNo** - Number of threads used to push data to the message queue service
- **DataAcquisition_RMQUseSSL** - Use secure sockets layer (SSL) - for secure traffic encryption
- **DataAcquisition_RMQ_host** - Hostname or IP of the message queue server (may differ from the database server in distributed setups)
- **DataAcquisition_RMQ_password** - Password for message queue service authentication
- **DataAcquisition_RMQ_port** - Port used by the message queue service
- **DataAcquisition_RMQ_queue** - The messaging queue name for queuing services
- **DataAcquisition_RMQ_username** - Administrative username for the message queue service
- **DataAcquisition_run_collection_servers** - Boolean flag indicating whether to run collection servers (used in cluster deployments)
- **DataAcquisition_sendRawData** - Determines whether raw data is sent to short-term storage (Online DataStorage)
- **DataAcquisition_ServiceDebugLevel** - Sets service logging verbosity: 0-FATAL ERROR, 1-WARNING, 2-INFO, 3-DEBUG
- **DataAcquisition_supressRawData** - Determines whether raw data is deleted to send to long-term storage (datastorage)
- **DataAcquisition_throttle_queue** - Defines the maximum number of events allowed in the message queue before event transmission stops. Once this limit is reached, all subsequent events are cached locally
- **DataAcquisition_UseDefaultParsers** - Enables internal parsers for all incoming events
- **DataAcquisition_use_http_ES_DA_client** - Determines whether HTTP transport is used for short-term storage (Elasticsearch). If set to false, data is transmitted using alternative methods via the queue service (fanout)
- **DataAcquisition_validateDataForEL** - Validates data before sending it to Elasticsearch
- **DataAcquisition_writeEventPath** - Path used to send events within CYBERQUEST to short-term storage (Online DataStorage)

Data Correlation

Select the **DataCorrelation** entry to configure parameters related to data correlation. This section allows updating all parameters related to data correlation.

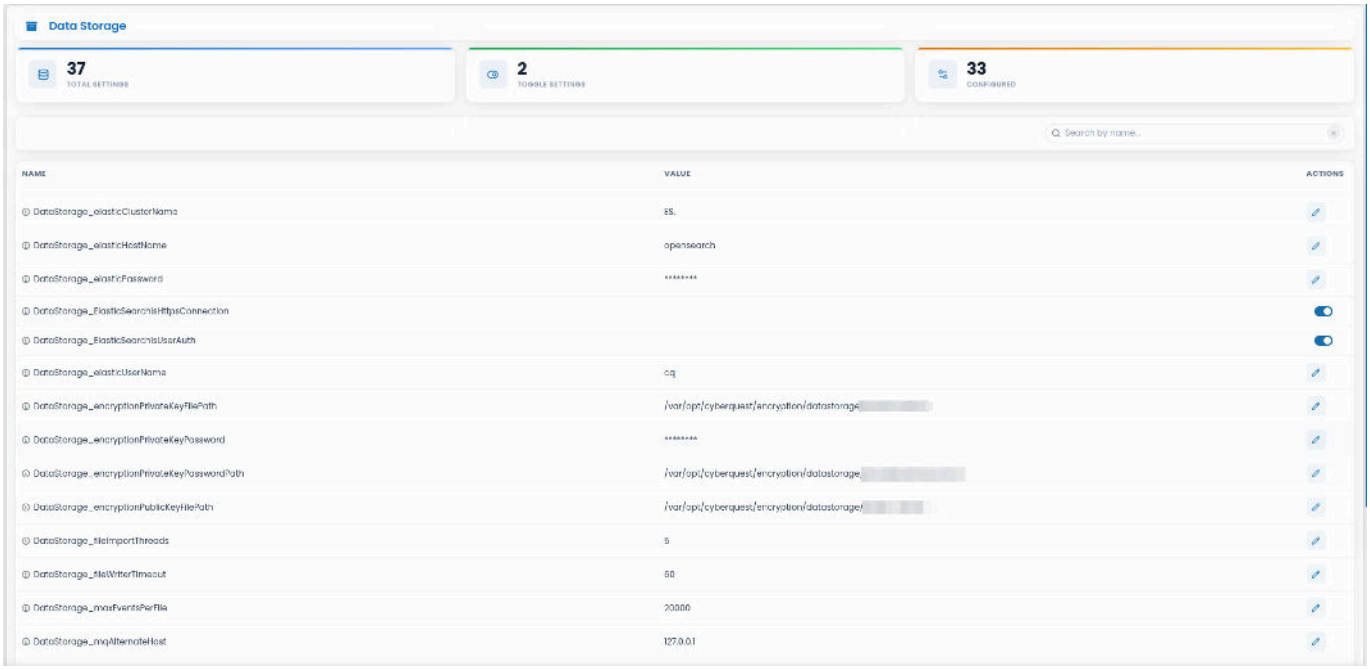


- **DataCorrelation_AplicationGUID** - The server's globally unique identifier, represented as 32 hexadecimal digits (lowercase or uppercase) in the format `8-4-4-4-12`, totaling 36 characters
- **DataCorrelation_cache_path** - Filesystem location where correlation cache files are stored
- **DataCorrelation_DebugLevel** - Sets the debug logging level:
  - 0 - FATAL ERROR, ERROR messages
  - 1 - WARNING messages
  - 2 - INFO messages
  - 3 - DEBUG messages
- **DataCorrelation_ElasticSearchIsHttpsConnection** - HTTPS connections of Online DataStorage
- **DataCorrelation_EL_Port** - Short-term storage (Online DataStorage) port
- **DataCorrelation_ElasticSearchPassword** - Password for authenticating with Online DataStorage
- **DataCorrelation_ElasticSearchUseAuthentication** - Enables authentication when connecting to Online DataStorage
- **DataCorrelation_ElasticSearchUsername** - Username for authenticating with Online DataStorage
- **DataCorrelation_EL_Url** - Short term storage (Online DataStorage) address
- **DataCorrelation_MetricsHostnameTag** - Hostname label included in correlation metrics to identify the source system in monitoring tools
- **DataCorrelation_MetricsHostTag** - Custom tag used in correlation metrics for distinguishing data from specific hosts or environments
- **DataCorrelation_MetricsServerAddress** - IP address or hostname of the metrics server that collects and stores correlation metrics
- **DataCorrelation_MetricsServerEnable** - Boolean setting that enables or disables sending correlation metrics to the metrics server
- **DataCorrelation_MetricsServerPort** - Network port on the metrics server used to receive correlation metrics
- **DataCorrelation_PercolatorNumberOfContainers** - Number of containers used by the percolator for correlation processing
- **DataCorrelation_PercolatorThreadPoolSize** - Number of threads allocated in the thread pool for percolator operations
- **DataCorrelation_RedisServerPORT** - Memory based storage port
- **DataCorrelation_RedisServerURL** - Memory based storage address
- **DataCorrelation_restart** - Restarts the DataCorrelation service
- **DataCorrelation_RMQueueAddress** - Address of the messaging queue server. In distributed architectures, may differ from the database server.

- **DataCorrelation_RMQueueName** - The messaging queue name for queuing services
- **DataCorrelation_RMQueuePassword** - Password for authenticating with the messaging queue service
- **DataCorrelation_RMQueuePort** - Port used by the messaging queue service
- **DataCorrelation_RMQueueUserName** - Username for authenticating with the messaging queue service
- **DataCorrelation_RMQUseSSL** - Enables SSL encryption for secure traffic with the messaging queue service
- **DataCorrelation_throttle_queue** - Throttle value

Data Storage

Access the **DataStorage** entry to modify parameters related to how data is stored and managed within the system.

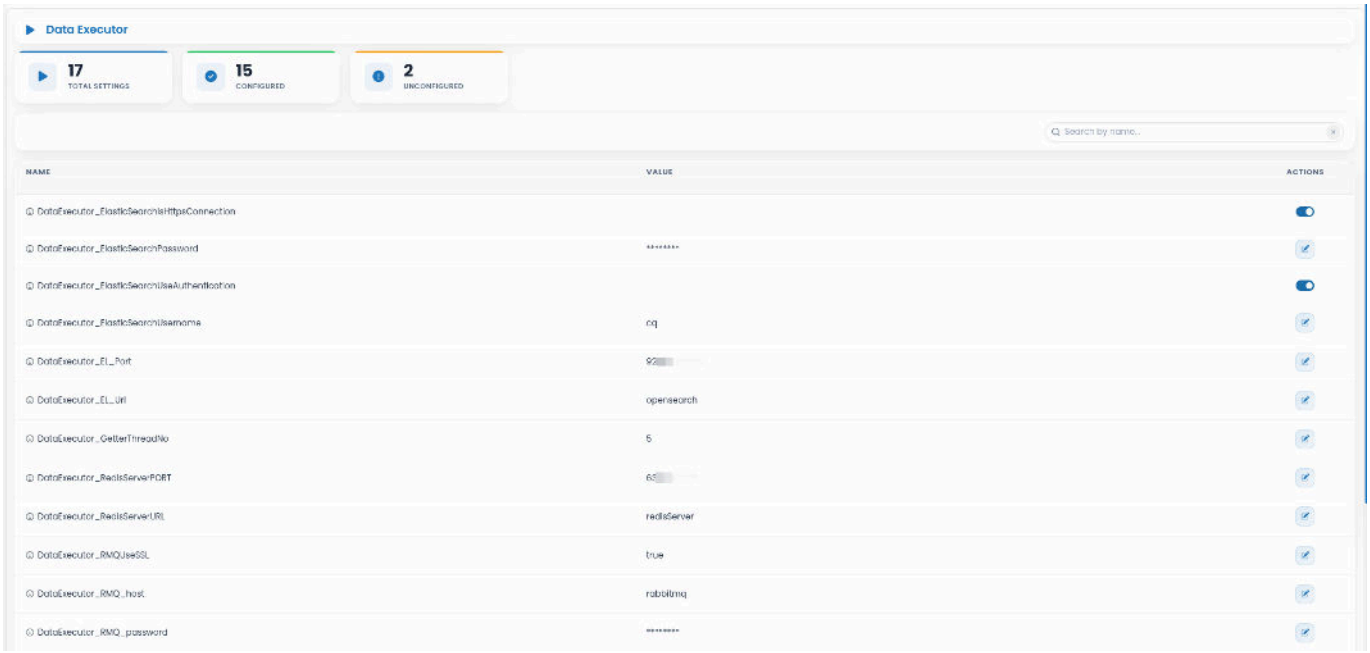


- **DataStorage_elasticClusterName** - Name of the Online DataStorage cluster
- **DataStorage_elasticHostName** - Hostname of the Online DataStorage server
- **DataStorage_elasticPassword** - Password for accessing Online DataStorage
- **DataStorage_ElasticSearchIsHttpsConnection** - HTTPS connections of Online DataStorage
- **DataStorage_ElasticSearchIsUserAuth** - Indicates whether user authentication is required for Online DataStorage
- **DataStorage_elasticUserName** - Username for accessing Online DataStorage
- **DataStorage_encryptionPrivateKeyFilePath** - File path of the defined private key
- **DataStorage_encryptionPrivateKeyPassword** - Password for the defined private key
- **DataStorage_encryptionPrivateKeyPasswordPath** - File path where the private key password is stored
- **DataStorage_encryptionPublicKeyFilePath** - File path of the defined public key
- **DataStorage_fileImportThreads** - Number of threads used for file import operations
- **DataStorage_fileWriterTimeout** - Timeout interval for the event writer process
- **DataStorage_maxEventsPerFile** - Maximum number of events allowed stored file
- **DataStorage_mqAlternateHost** - Alternate MQ host used if the primary host becomes unavailable
- **DataStorage_mqExchangeName** - Exchange name used by the MQ service
- **DataStorage_mqHost** - MQ service host. In distributed architectures, it may differ from the default CYBERQUEST server
- **DataStorage_mqPassword** - Password for MQ service access
- **DataStorage_mqPort** - Communication port used by the MQ service
- **DataStorage_mqQueueName** - Name of the MQ queue
- **DataStorage_mqQueueType** - Type of MQ queue
- **DataStorage_mqReceiveCommandExchangeName** - Exchange name for MQ receive commands
- **DataStorage_mqReceiveCommandQueueName** - Queue name for MQ receive commands
- **DataStorage_mqReceiveCommandQueueType** - Queue type for MQ receive commands
- **DataStorage_mqReceiveCommandRouting** - Routing path for MQ receive commands

- **DataStorage_mqReceiveExchangeName** - Exchange name for MQ receive operations
- **DataStorage_mqReceiveQueueName** - Queue name for MQ receive operations
- **DataStorage_mqReceiveQueueType** - Queue type for MQ receive operations
- **DataStorage_mqReceiveRouting** - Routing key for MQ receive operations
- **DataStorage_mqRouting** - General routing path for message queues
- **DataStorage_mqSendExchangeName** - Exchange name for MQ send operations
- **DataStorage_mqSendQueueName** - Queue name for MQ send operations
- **DataStorage_mqSendQueueType** - Queue type for MQ send operations
- **DataStorage_mqSendRouting** - Routing path for MQ send operations
- **DataStorage_mqUserName** - Administrative username for accessing MQ services
- **DataStorage_mqVHost** - MQ service virtual host. In distributed architectures, it may differ from the default CYBERQUEST server

Data Executor

Select the **Data Executor** entry to configure parameters related to data executor. This section allows updating all parameters related to data executor.

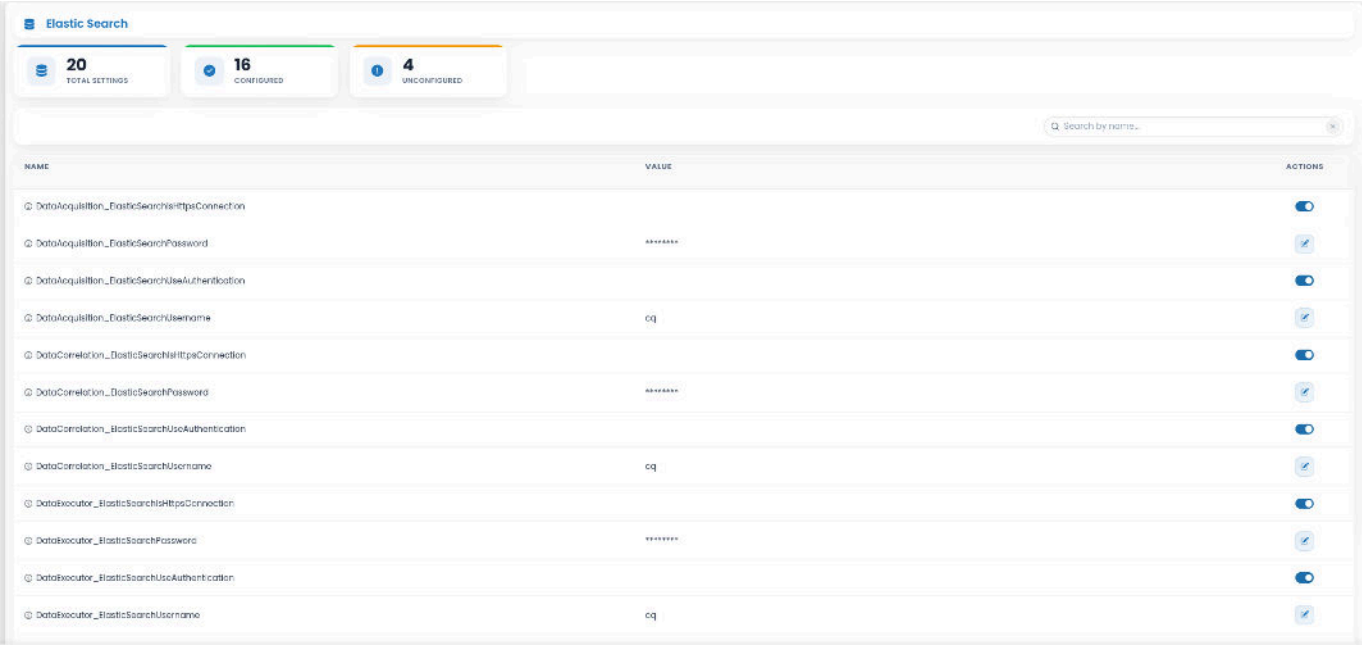


- **DataExecutor_ElasticSearchIsHttpsConnection** - HTTPS connections of Online DataStorage
- **DataExecutor_ElasticSearchPassword** - Password for authenticating with Online DataStorage
- **DataExecutor_ElasticSearchUseAuthentication** - Enables authentication when connecting to Online DataStorage
- **DataExecutor_ElasticSearchUsername** - Username for authenticating with Online DataStorage
- **DataExecutor_EL_Port** - Short-term storage (Online DataStorage) port
- **DataExecutor_EL_Url** - Short term storage (Online DataStorage) address
- **DataExecutor_GetterThreadNo** - Number of threads used by the Data Executor to retrieve data from storage or queues
- **DataExecutor_RedisServerPORT** - Memory based storage port
- **DataExecutor_RedisServerURL** - Memory based storage address
- **DataExecutor_RMQUseSSL** - Use secure sockets layer (SSL) - for secure traffic encryption
- **DataExecutor_RMQ_host** - Hostname or IP address of the RabbitMQ server
- **DataExecutor_RMQ_password** - Password for connecting to RabbitMQ
- **DataExecutor_RMQ_port** - Port used by the message queue service
- **DataExecutor_RMQ_queue** - Name of the RabbitMQ queue from which the Data Executor retrieves tasks
- **DataExecutor_RMQ_username** - Username for RabbitMQ authentication
- **DataExecutor_ServiceDebugLevel** - Sets service logging verbosity: 0-FATAL ERROR, 1-WARNING, 2-INFO, 3-DEBUG

- **DataExecutor_V8EngineTimeout** - Maximum execution time (in milliseconds) allowed for scripts running in the V8 JavaScript engine before being stopped automatically.

Elastic Search

Select **ElasticSearch** to modify NoSQL configuration parameters. This section contains all settings related to the Online DataStorage nodes and search engine behavior.



- **DataAcquisition_ElasticSearchIsHttpsConnection** - HTTPS connections of Online DataStorage
- **DataAcquisition_ElasticSearchPassword** - Password for authenticating with Online DataStorage
- **DataAcquisition_ElasticSearchUseAuthentication** - Authentication for connecting to Online DataStorage
- **DataAcquisition_ElasticSearchUsername** - Username for authenticating with Online DataStorage
- **DataCorrelation_ElasticSearchIsHttpsConnection** - HTTPS connections of Online DataStorage
- **DataCorrelation_ElasticSearchPassword** - Password for authenticating with Online DataStorage
- **DataCorrelation_ElasticSearchUseAuthentication** - Enables authentication when connecting to Online DataStorage
- **DataCorrelation_ElasticSearchUsername** - Username for authenticating with Online DataStorage
- **DataExecutor_ElasticSearchIsHttpsConnection** - HTTPS connections of Online DataStorage
- **DataExecutor_ElasticSearchPassword** - Password for authenticating with Online DataStorage
- **DataExecutor_ElasticSearchUseAuthentication** - Enables authentication when connecting to Online DataStorage
- **DataExecutor_ElasticSearchUsername **- Username for authenticating with Online DataStorage
- **DataStorage_ElasticSearchIsHttpsConnection** - HTTPS connections of Online DataStorage
- **DataStorage_ElasticSearchIsUserAuth** - Indicates whether user authentication is required for Online DataStorage
- **ElasticSearchIsHttpsConnection** - Online DataStorage is Https Connection
- **ElasticSearchPassword** - Online DataStorage password
- **ElasticSearchPort** - Port number used for connecting to Online DataStorage.
- **ElasticSearchServer** - Hostname or IP address of the Online DataStorage server
- **ElasticSearchUseAuthentication** - Enables or disables authentication for Online DataStorage connections
- **ElasticSearchUsername** - Username for Online DataStorage authentication

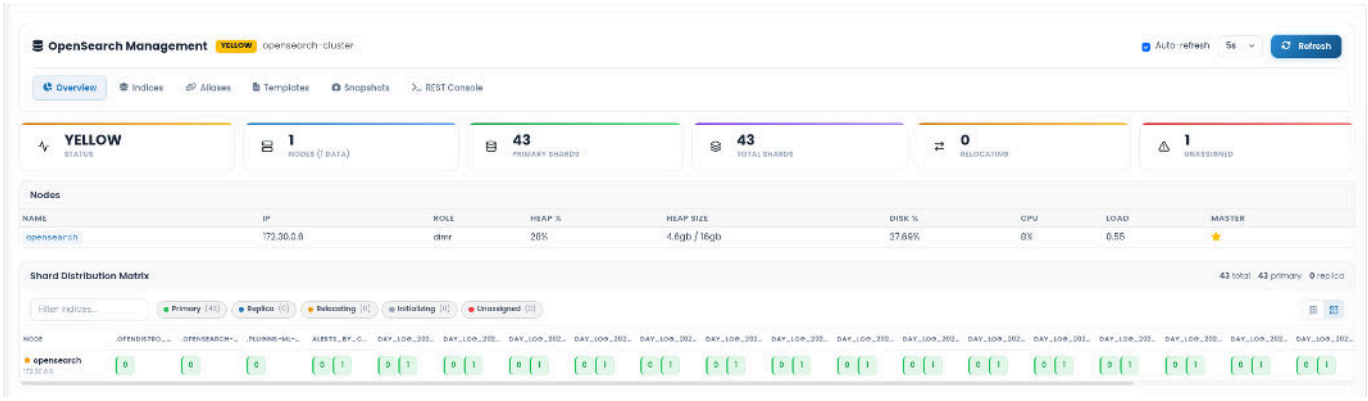
OpenSearch Management

The **OpenSearch Management** section provides an administrative interface for monitoring and managing the OpenSearch cluster used by CYBERQUEST.

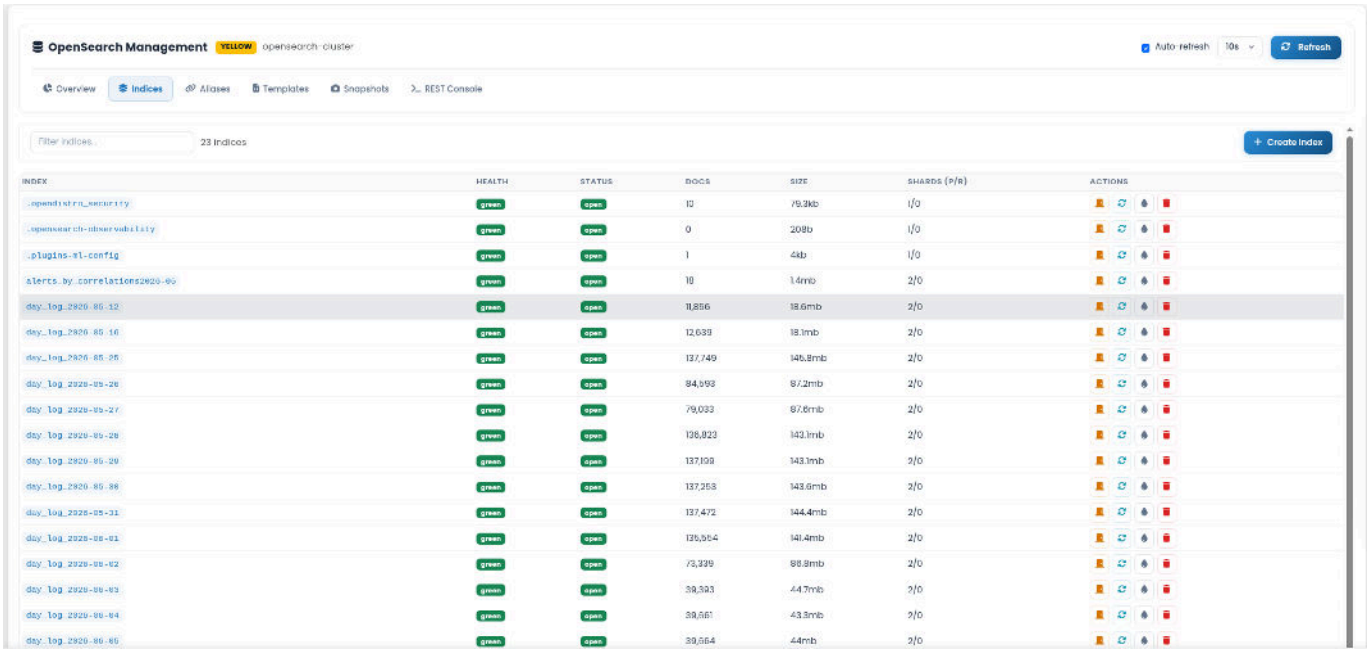
The OpenSearch Management interface displays the current cluster health status, such as **GREEN**, **YELLOW** or **RED** together with the configured cluster name. The page can be refreshed manually using the **Refresh** button, or automatically by enabling **Auto-refresh** and selecting the desired refresh interval.

The following views are available:

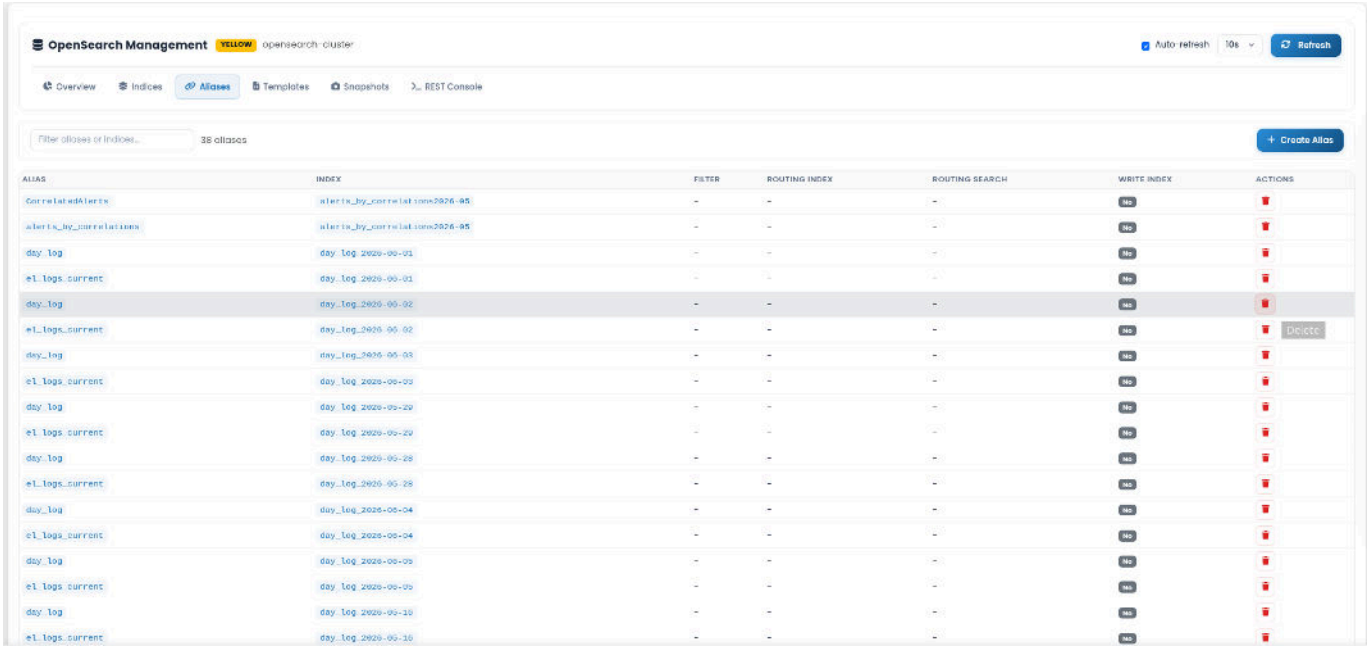
- **Overview** - Displays general cluster health information, including cluster status, number of nodes, primary shards, total shards, relocating shards, and unassigned shards. It also shows node-level information such as IP address, role, heap usage, disk usage, CPU, load, and master node status.



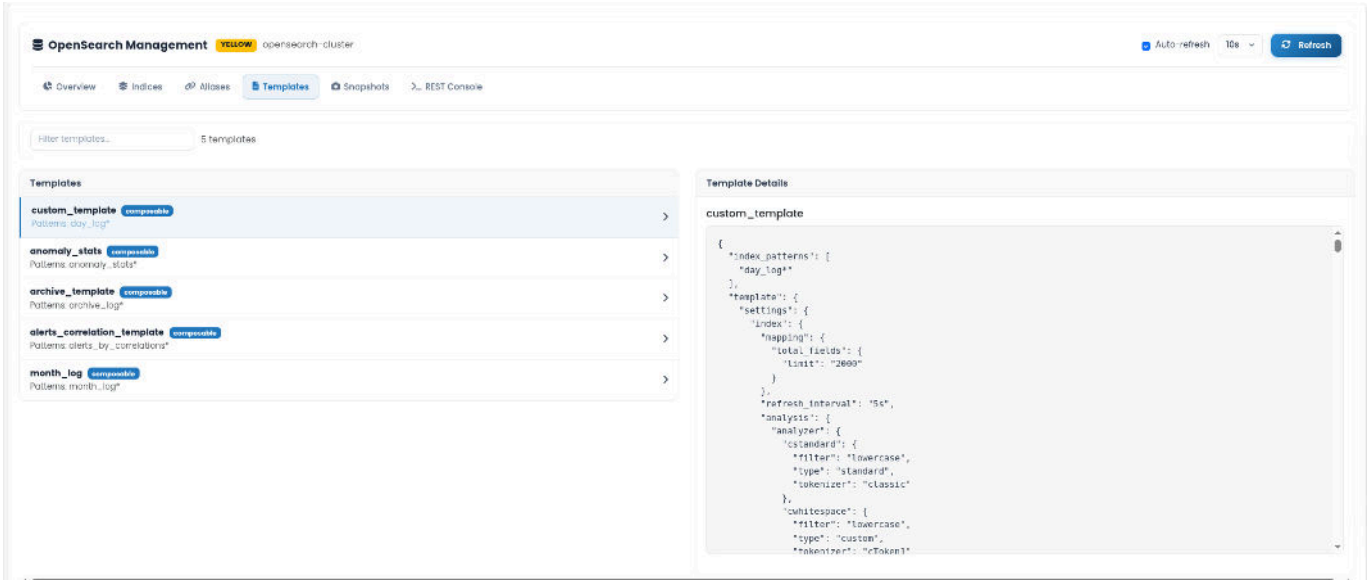
- **Indices** - Displays the list of OpenSearch indices, including index name, health, status, document count, size, and shard allocation. From this view, administrators can review index status and perform available index actions.



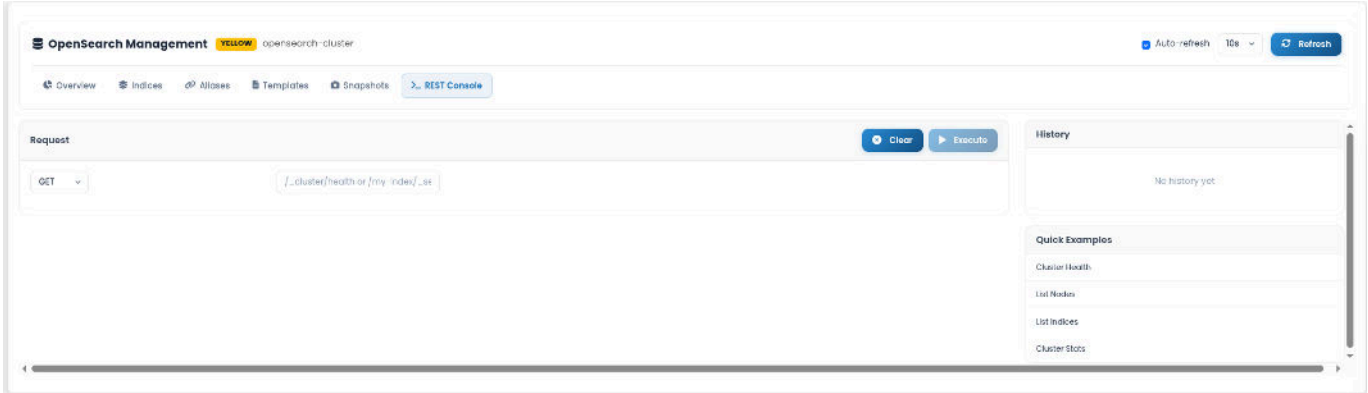
- **Aliases** - Displays configured aliases and the indices they point to. This helps administrators verify which aliases are used for querying or routing data across different indices.



- **Templates** - Displays available index templates and their configuration details. Templates define index patterns, mappings, settings, and other rules applied when matching indices are created.



- **Snapshots** - Provides access to snapshot-related information used for backup and restore operations, depending on the configured OpenSearch environment.
- **REST Console** - Allows administrators to execute OpenSearch REST API requests directly from the CYBERQUEST interface. This can be used to check cluster health, list nodes, list indices, review cluster statistics, or run other supported API calls.



Reports Customization

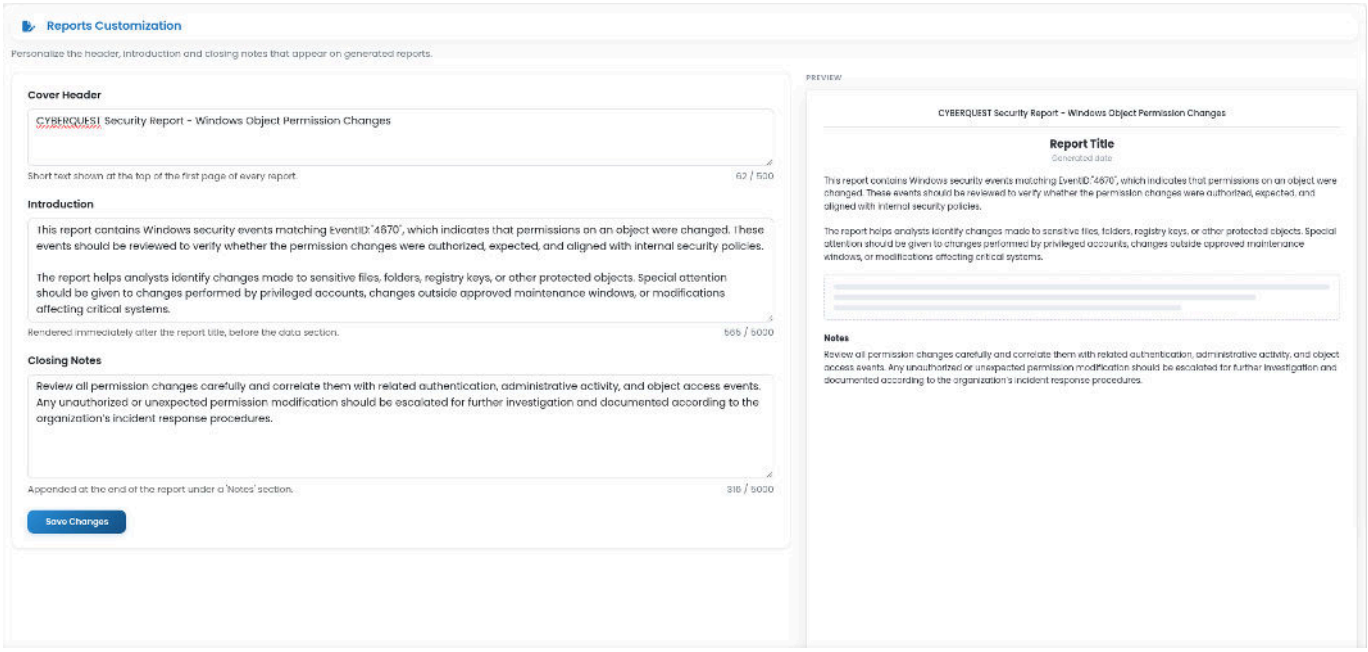
The **Reports Customization** section allows administrators to personalize the text displayed in generated reports. This includes the report cover header, introduction, and closing notes, helping organizations add context, internal guidance, or reporting instructions to exported reports.

To access this section, go to **Settings > Application Settings > Data & Storage > Reports Customization**.

The following fields are available:

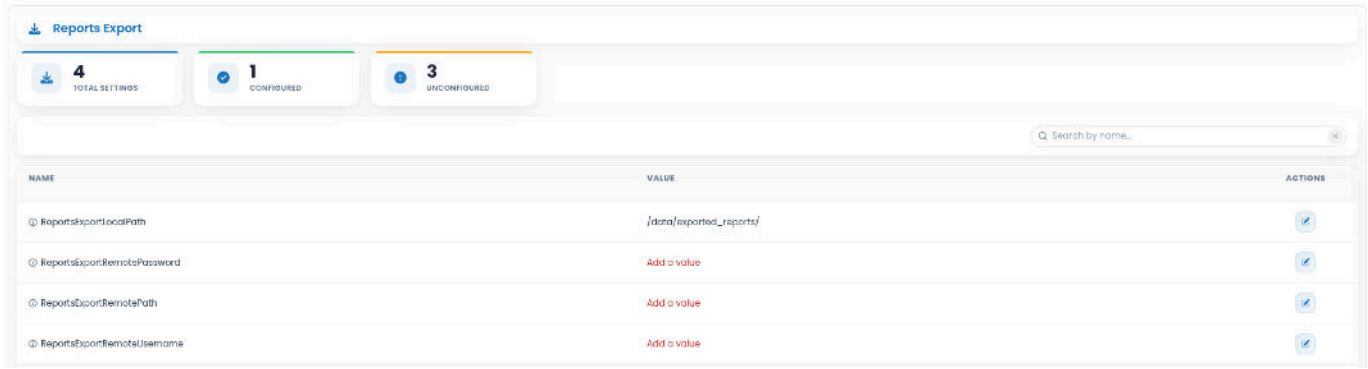
- **Cover Header** - Defines a short header displayed at the top of the first page of each generated report. This can be used for the organization name, report category, or a short report label.
- **Introduction** - Defines the text displayed after the report title and before the report data. This section can describe the purpose of the report, the type of events included, and the review context.
- **Closing Notes** - Defines the notes displayed at the end of the report under the **Notes** section. This field can be used to include investigation guidance, escalation instructions, or internal review recommendations.

The **Preview** panel on the right side shows how the configured text will appear in the generated report. After updating the required fields, click **Save Changes** to apply the configuration.



Reports Export

Select **ReportsExport** to modify the configuration settings for report exports. This section contains all parameters related to the generation and export of reports.

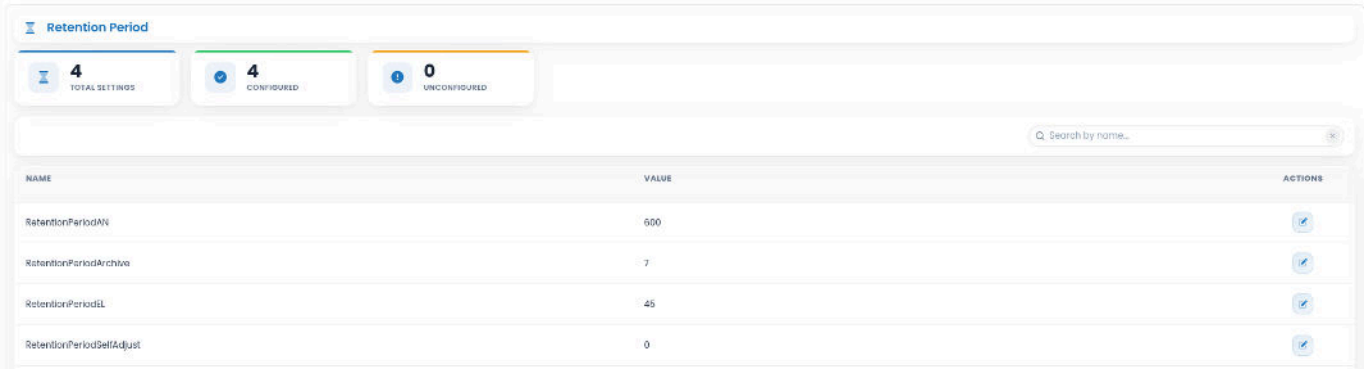


- **ReportsExportLocalPath** - The directory path on the local system where generated reports are stored before export.
- **ReportsExportRemotePassword** - The authentication password used to connect to the remote server for report export.
- **ReportsExportRemotePath** - The directory path on the remote server where exported reports will be stored.

- **ReportsExportRemoteUsername** - The username used to authenticate with the remote server for report export.

Retention Period

Select **RetentionPeriod** to modify the duration for which stored data is retained. This section contains all parameters related to data retention management.



- **RetentionPeriodAN:** Specifies the retention duration for data in the Data Analyzer *(Deprecated)*.
- **RetentionPeriodArchive:** Defines how long unarchived data is kept when using the **Archives** option in jobs.

For instructions on importing data from an archive, refer to: How to import data from archive

- **RetentionPeriodEL:** Determines the retention policy for the online data and online repository (Online DataStorage).
- **RetentionPeriodSelf Adjust:** Accepts values **1** (ON) or **0** (OFF).

1 (ON) - The retention period in the online database (Elasticsearch) is automatically adjusted based on the allocated storage capacity.

0 (OFF) - The value in **RetentionPeriodEL** remains fixed. CYBERQUEST will continue collecting data until disk space is full, after which no new data will be collected.

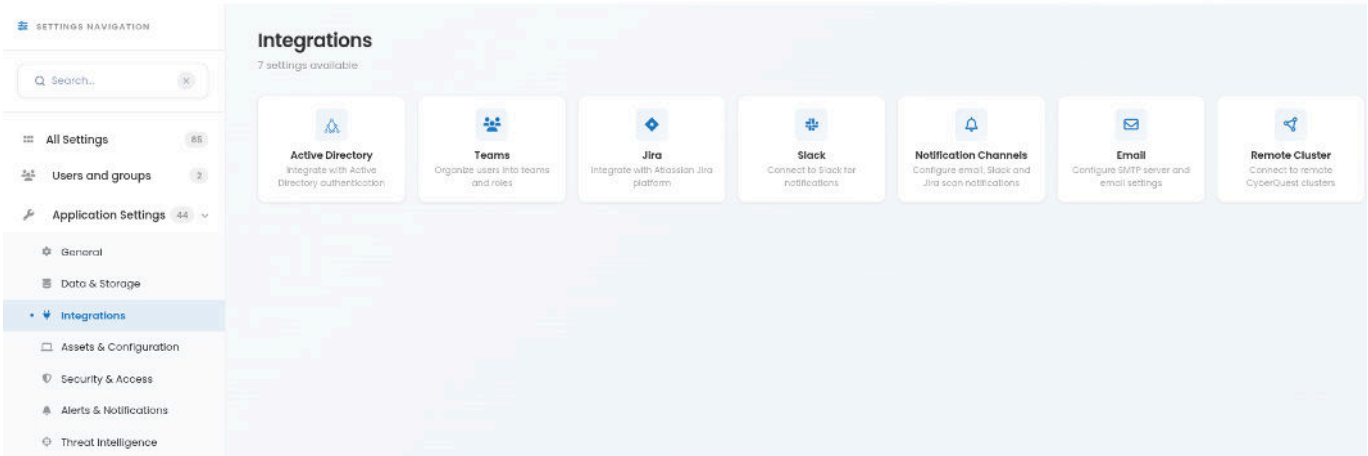
Data Storages

Provides access to storage-related configuration areas used to manage how CYBERQUEST collects, processes, and stores data. For detailed configuration instructions, including storage settings, message queues, encryption options, and external storage integrations, refer to the Data Storages.

Integrations

The **Integrations** section provides access to configuration areas used to connect CYBERQUEST with external systems, identity providers, collaboration platforms, notification services, and remote CYBERQUEST clusters.

To access this section, go to **Settings > Application Settings > Integrations**.



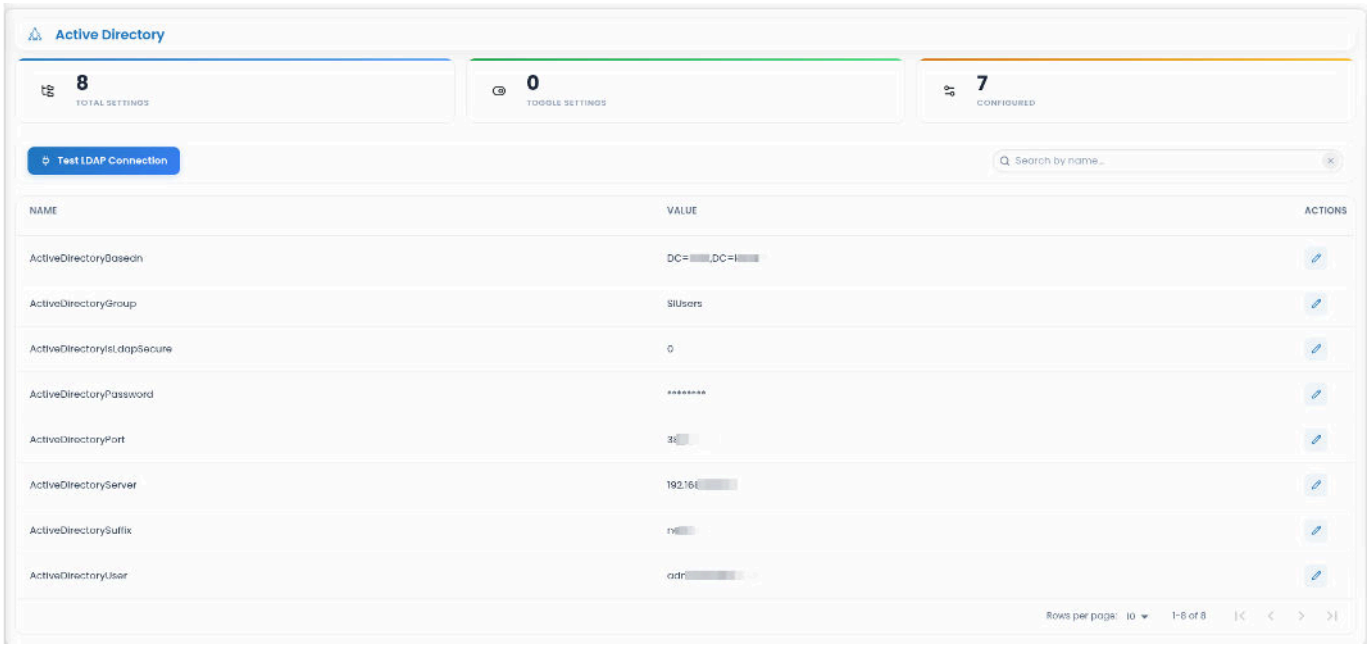
The available options include:

- **Active Directory** - Configures integration with Active Directory, allowing users from selected AD groups to authenticate in CYBERQUEST using their AD credentials.
- **Teams** - Configures Microsoft Teams integration settings used for collaboration and notification workflows.
- **Jira** - Configures Jira integration settings for ticketing, issue tracking, and workflow management.
- **Slack** - Configures Slack integration settings used for notifications and team communication.
- **Notification Channels** - Defines notification delivery channels, such as email, Slack, or Jira, used by CYBERQUEST to send alerts and scan-related notifications.
- **Email** - Configures email delivery settings, including the parameters required for CYBERQUEST to send emails, notifications, and reports.
- **Remote Cluster** - Configures connections between multiple CYBERQUEST instances, enabling federated search across distributed environments.

Active Directory

A dedicated section for configuring CYBERQUEST integration with Active Directory.

Through this integration, an Active Directory group can be assigned access rights, allowing its members to authenticate in CYBERQUEST using their AD credentials.

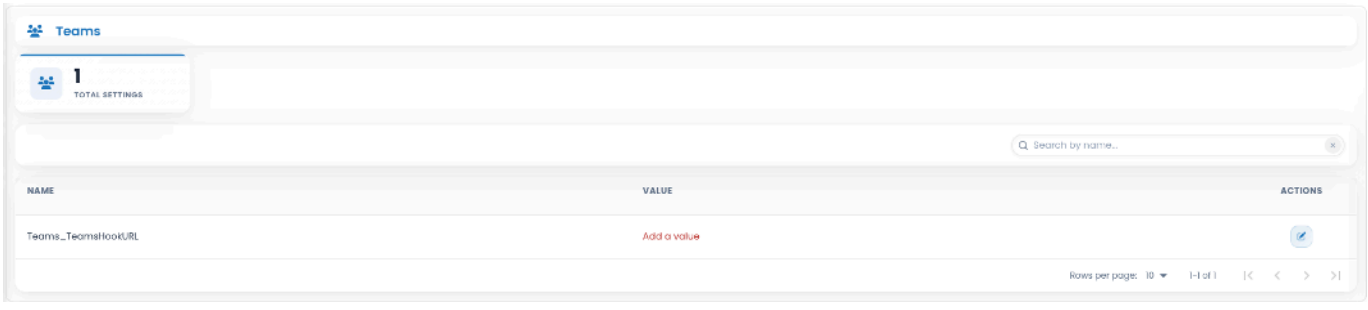


To see more information about Active Directory, please check the links below:

- How to collect data on Active Directory
- How to connect to Active Directory
- AD information needed to read AD objects

Teams

The **Teams** section is used to configure settings related to Microsoft Teams integration.



- Teams_TeamsHookURL - The webhook URL for the Microsoft Teams account where CYBERQUEST sends messages.

Jira

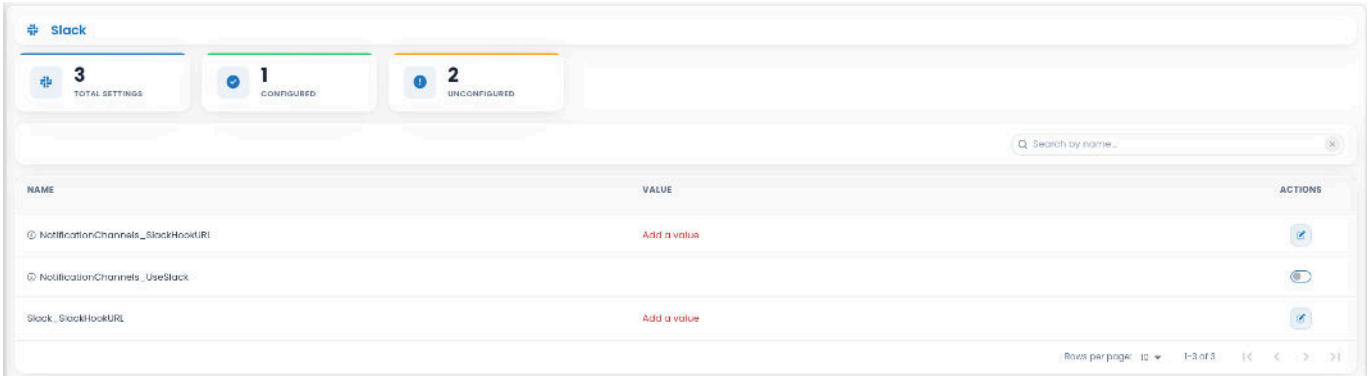
The **Jira** section is used to configure settings related to Jira integration.



- Jira_JiraHookURL - The webhook URL for the Jira account where CYBERQUEST sends messages.

Slack

The **Slack** section is used to configure settings related to Slack integration.



- Slack_SlackHookURL - The webhook URL for the Slack account where CYBERQUEST sends messages.

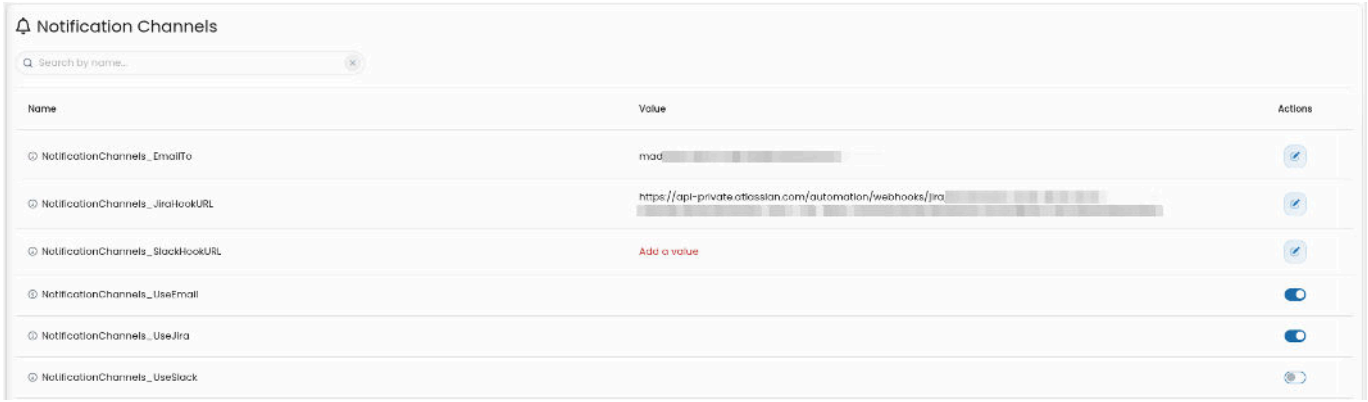
Notification Channels

The **Notification Channels** section allows administrators to configure the destinations used by CYBERQUEST for sending notifications.

To access this section, go to **Settings > Application Settings > Integrations > Notification Channels**.

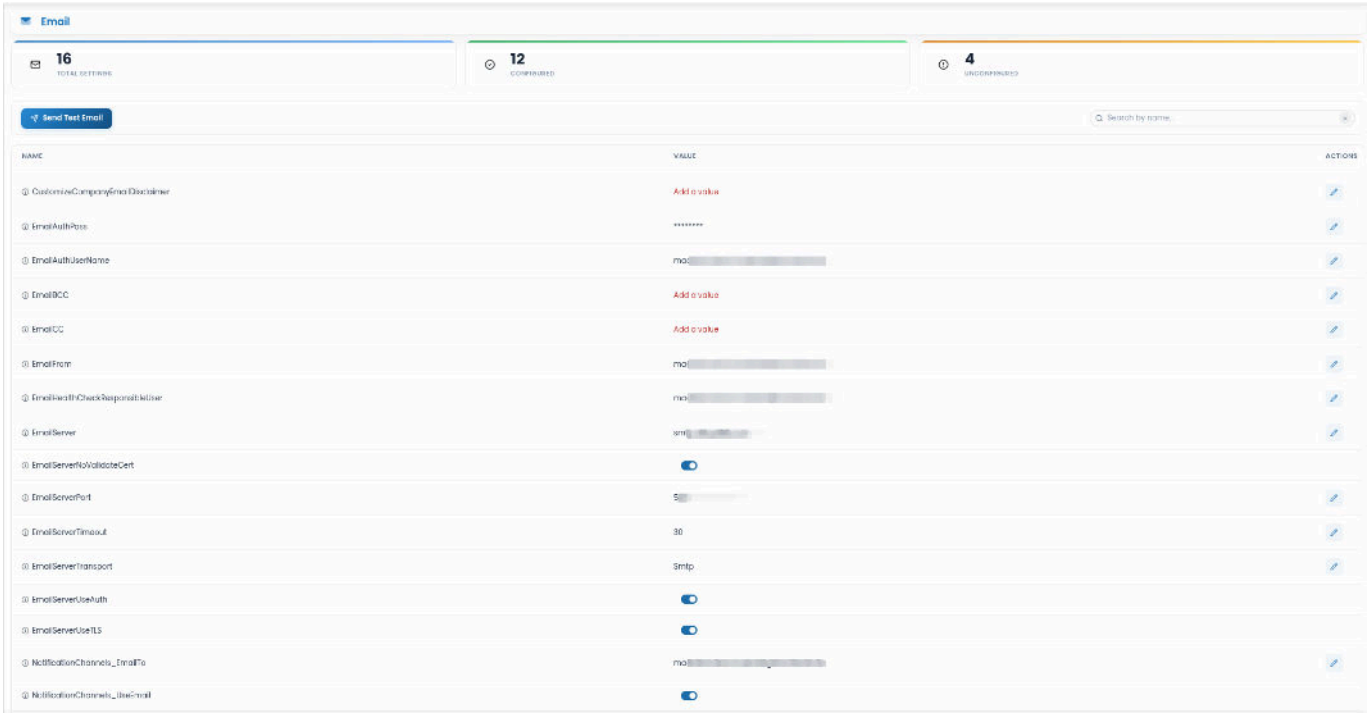
Available settings include:

- **NotificationChannels_EmailTo** - Defines the email address or list of email addresses used for notification delivery.
- **NotificationChannels_JiraHookURL** - Defines the Jira webhook URL used to send notifications or create/update Jira-related items.
- **NotificationChannels_SlackHookURL** - Defines the Slack webhook URL used to send notifications to a Slack channel.
- **NotificationChannels_UseEmail** - Enables or disables email notifications.
- **NotificationChannels_UseJira** - Enables or disables Jira notifications.
- **NotificationChannels_UseSlack** - Enables or disables Slack notifications.



Email

Select **Email** to configure parameters for email delivery in CYBERQUEST. This section includes all settings related to how CYBERQUEST sends emails.



- **CustomizeCompanyEmailDisclaimer** - Defines a custom email disclaimer or footer text to be appended to outgoing emails.
- **EmailAuthPass** - Password used for authentication with the outgoing email server
- **EmailAuthUserName** - Username used for authentication with the outgoing email server
- **EmailBCC** - One or more email addresses to receive BCC of all outgoing emails
- **EmailCC** - One or more email addresses to receive CC of all outgoing emails
- **EmailFrom** - The default "From" address displayed in emails sent by CYBERQUEST
- **EmailHealthCheckResponsibleUser** - The designated user who receives health check or system monitoring emails
- **EmailServer** - The hostname or IP address of the outgoing email server (SMTP server)
- **EmailServerNoValidateCert** - When enabled, bypasses validation of the server's SSL/TLS certificate
- **EmailServerPort** - The port used for communication with the outgoing email server
- **EmailServerTimeout** - The maximum time (in seconds) to wait for a response from the email server before timing out
- **EmailServerTransport** - The communication protocol used to send emails (e.g., SMTP, SMTPS)
- **EmailServerUseAuth** - Indicates whether authentication is required to connect to the outgoing email server
- **EmailServerUseTLS** - Specifies whether to use TLS encryption when sending emails
- **NotificationChannels_EmailTo** - Defines the email recipient address or addresses used for sending CYBERQUEST notifications.

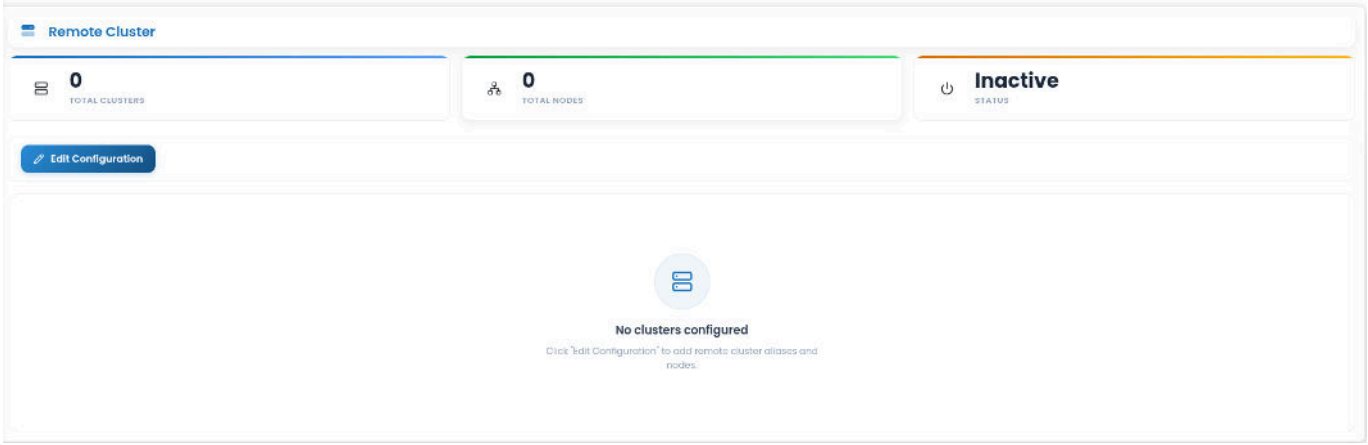
- **NotificationChannels_UseEmail** - Enables or disables email notifications. When enabled, CYBERQUEST can send notifications to the configured email recipients.

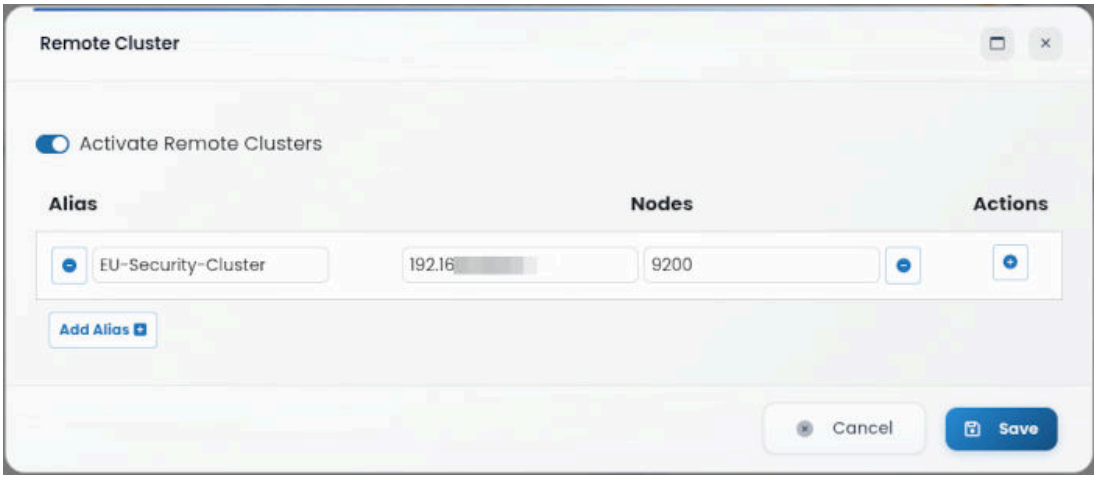
Remote Cluster

Select **Remote Cluster** to configure connections between multiple CYBERQUEST instances, enabling federated search capabilities across distributed environments. This feature enables federated search, allowing the local CYBERQUEST instance to query data from one or more remote clusters and return results from distributed environments in a unified way.

The **Remote Cluster** page displays the current configuration status, including the total number of configured clusters, the total number of nodes, and whether remote cluster functionality is active or inactive. If no clusters are configured, the page displays an empty state message and prompts the user to edit the configuration.

To configure a remote cluster, click **Edit Configuration**. This opens the remote cluster configuration window.





The following options are available:

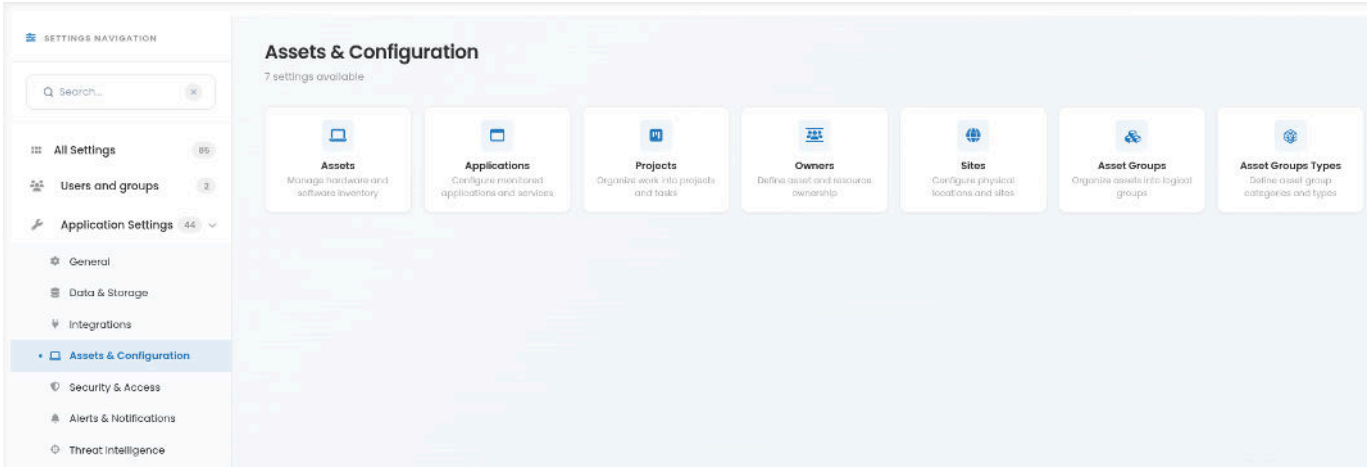
- **Activate Remote Clusters** - Enables or disables remote cluster connections.
- **Alias** - Name of the remote cluster.
- **Nodes** - Remote cluster node details.
- **IP Address / Hostname** - Address of the remote cluster node.
- **Port** - Communication port for the remote cluster node.
- **Add Alias** - Adds a new remote cluster configuration.

After adding the required cluster details, click **Save** to apply the configuration or **Cancel** to discard the changes.

Assets & Configuration

The **Assets & Configuration** section provides access to configuration areas for managing assets, monitored applications, projects, ownership, sites, and asset grouping within CYBERQUEST.

To access this section, go to **Settings > Application Settings > Assets & Configuration**.



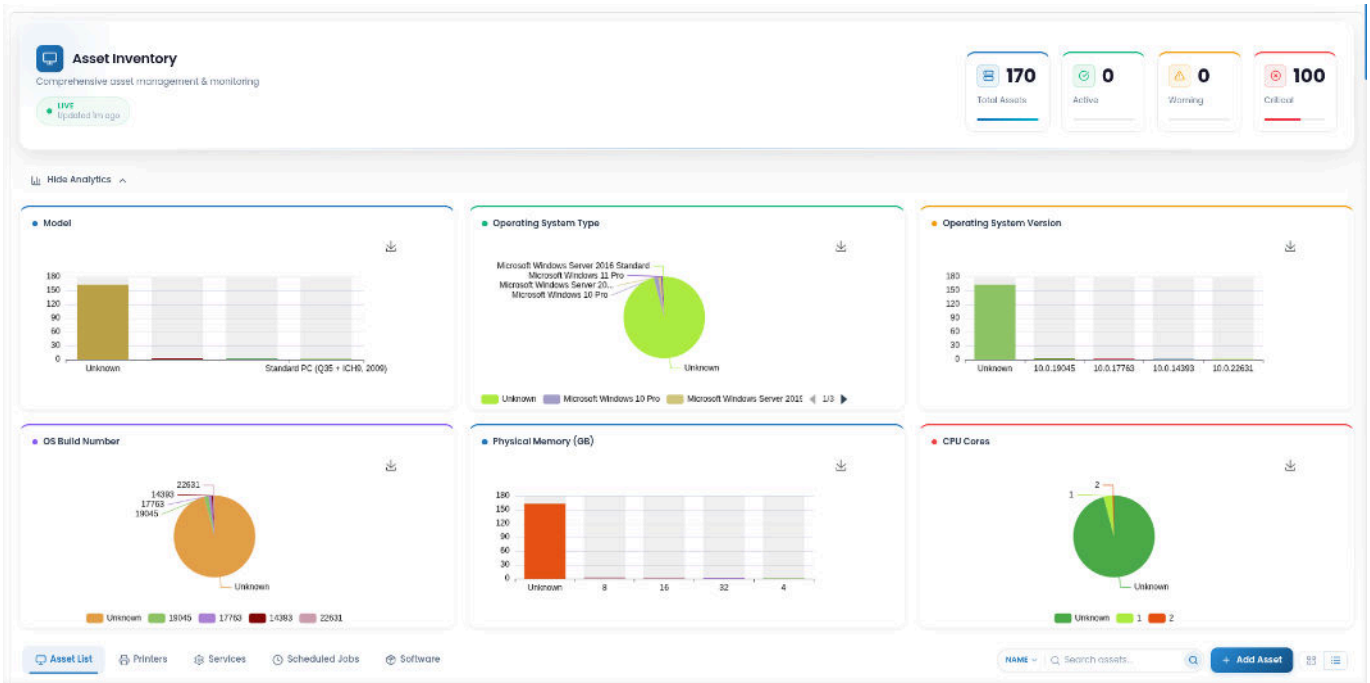
The available options include:

- **Assets** - Manages asset inventory. Asset details can be populated automatically as data is collected, while users can also manually add or update asset information.
- **Applications** - Configures and manages applications by defining their name, description, and purpose within the platform.
- **Projects** - Allows users to create and manage projects by defining their name, description, objectives, scope, or related activities.
- **Owners** - Defines owners responsible for assets, applications, or projects, helping clarify roles and areas of responsibility.
- **Sites** - Configures physical or logical locations by defining site names, descriptions, location details, or operational scope.
- **Asset Groups** - Organizes assets into logical groups and allows each group to be associated with a specific asset group type.
- **Asset Groups Types** - Defines the categories used to classify and organize asset groups.

Assets

Configuration page for assets. In the **Assets** module, details are automatically populated as data is collected, ensuring up-to-date information. Additionally, users can manually define new assets or modify existing asset details directly within the system, providing flexible and accurate asset management.

The **Assets** Settings section includes several visualizations including the *Asset Model, Operating System Types, Operating System Versions, OS Build Numbers, Physical Memory (in GB), and CPU Core counts.*

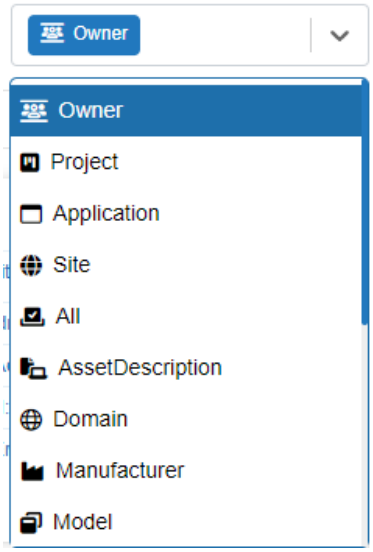




Additionally, this page provides a summary of assets grouped by the following categories: *ASSET LIST, PRINTERS, SERVICES, SCHEDULED JOBS,* and *SOFTWARE*.



On the right side of the page, a drop-down list allows grouping of assets by:

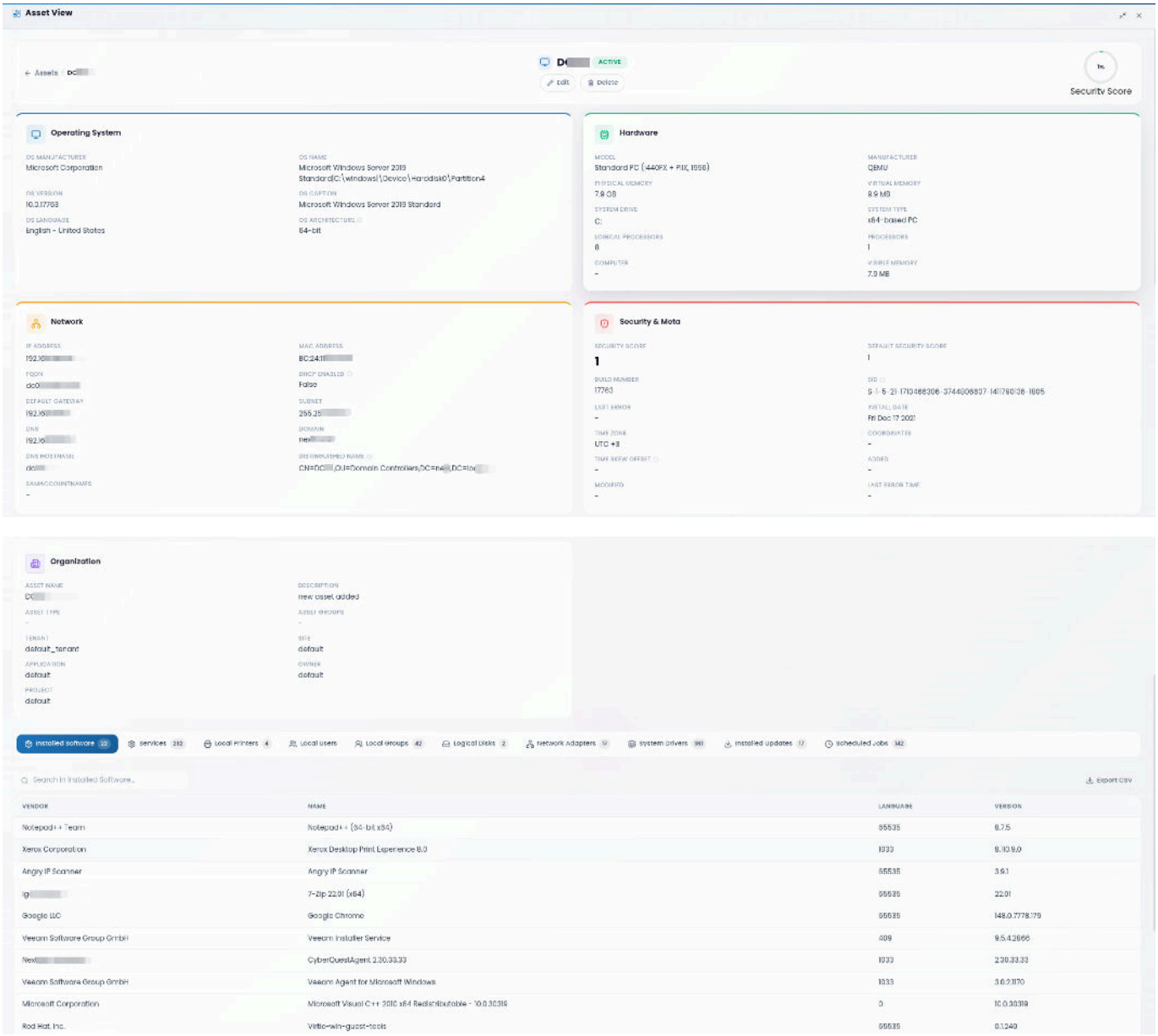


1. The **Asset List** contains all assets identified by CQ (Assets displaying a ***Last Error*** status need proper configuration to allow the CQ module to retrieve information). Options are available to Edit, Delete, or View each asset.

To view asset information, click the



button, which opens the detailed asset page:

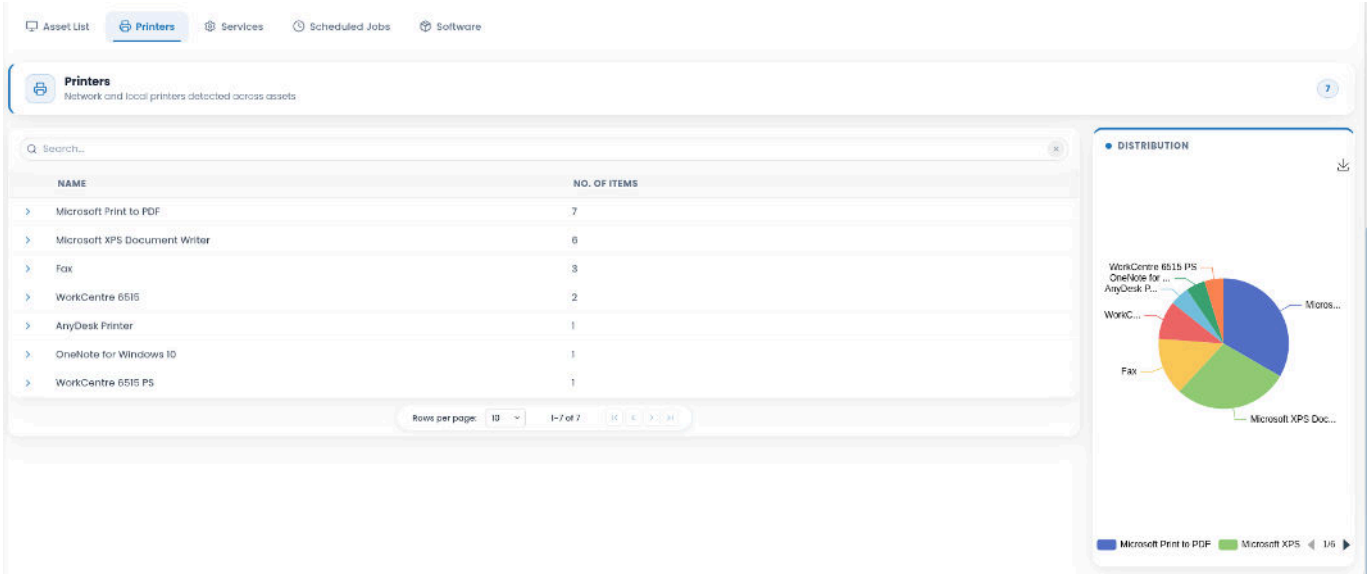


Expanding **Asset Details**, **Hardware Info**, and **Extended Info** reveals information about the Operating System, Network, and Hard Disk.

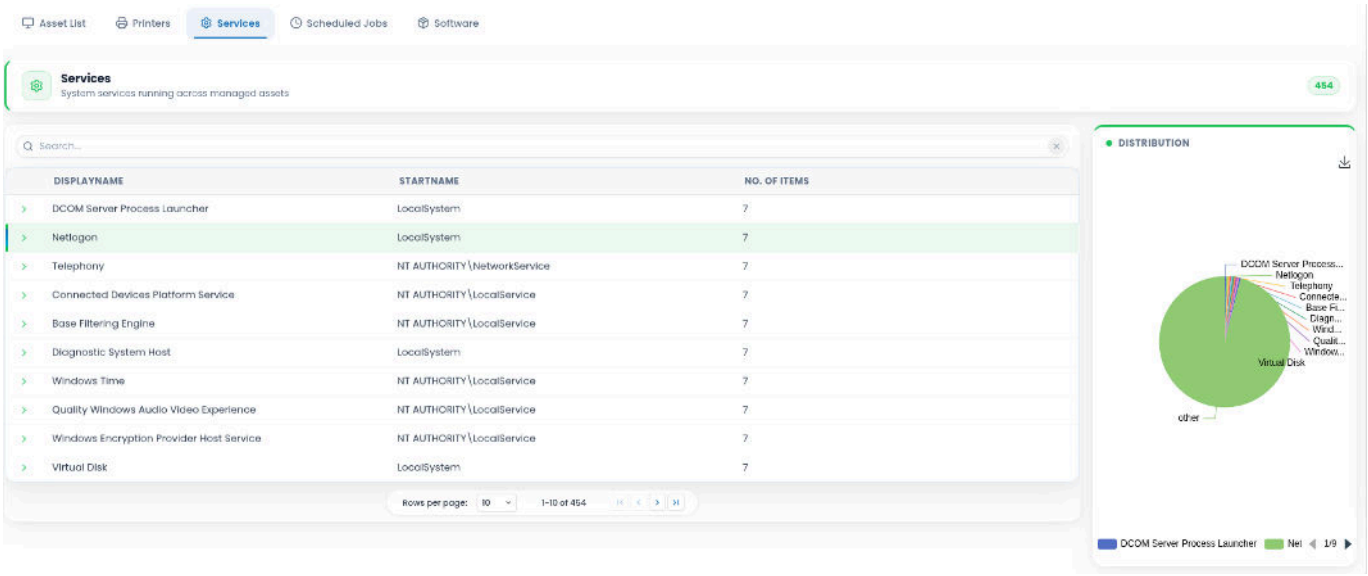
Within the fields section, the following information can be observed:

- *INSTALLED SOFTWARE* - software installed on the asset
- *SERVICES* - services present on the asset
- *LOCAL PRINTERS* - local printers associated with the asset
- *LOCAL USERS* - local users of the asset
- LOCAL GROUPS - local groups of the asset
- LOGICAL DISKS - partitions of the asset's physical disk
- *NETWORK ADAPTERS* - network adapters installed on the asset
- *DRIVERS* - drivers associated with the asset
- *INSTALLED UPDATES* - updates installed on the asset
- *SCHEDULED JOBS* - scheduled jobs configured for the asset

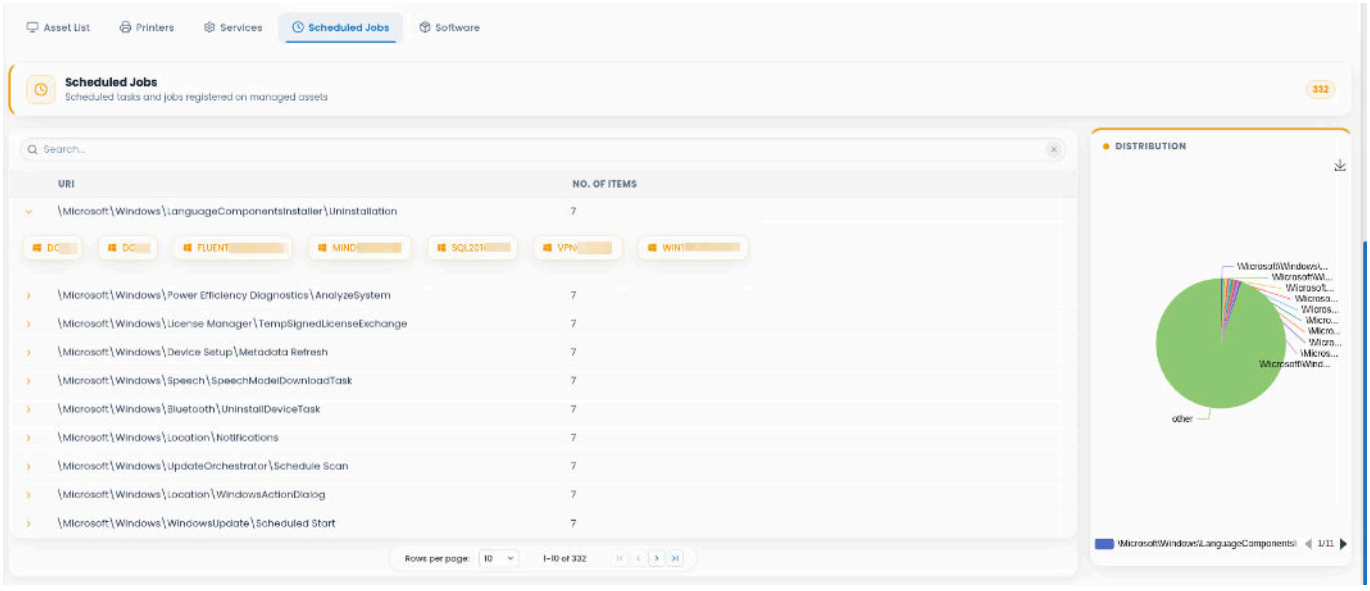
2.**Printers** - This section lists all printers identified by CQ, along with the number of assets associated with each printer (*e.g., the OneNote (Desktop) printer is found on 1 asset*).



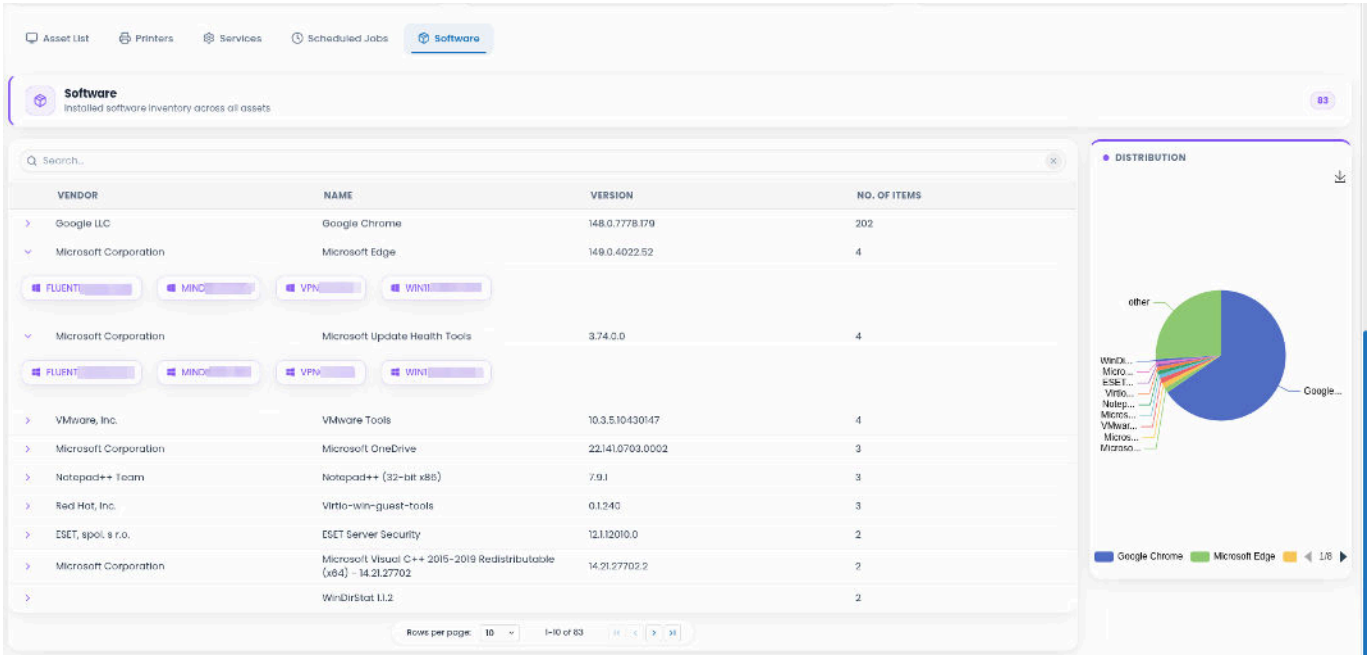
3.**Services** - This section displays all services identified by CQ, along with the number of assets associated with each service (*e.g., the Windows Remote Management (WS-Management) is found on 4 assets*).



4.**Scheduled Jobs** - This section lists all scheduled jobs identified by CQ, along with the number of assets associated with each job (*e.g., the Automatic-Device-Join scheduled job is found on 6 assets*).



5.**Software** - This section includes all software identified by CQ, along with the number of assets on which each software is installed (e.g., the software Next Generation Software is found on 2 assets).

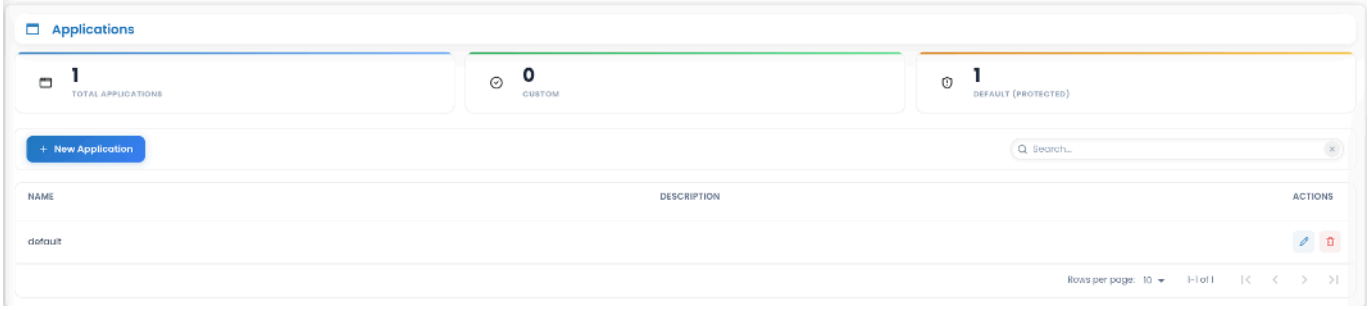


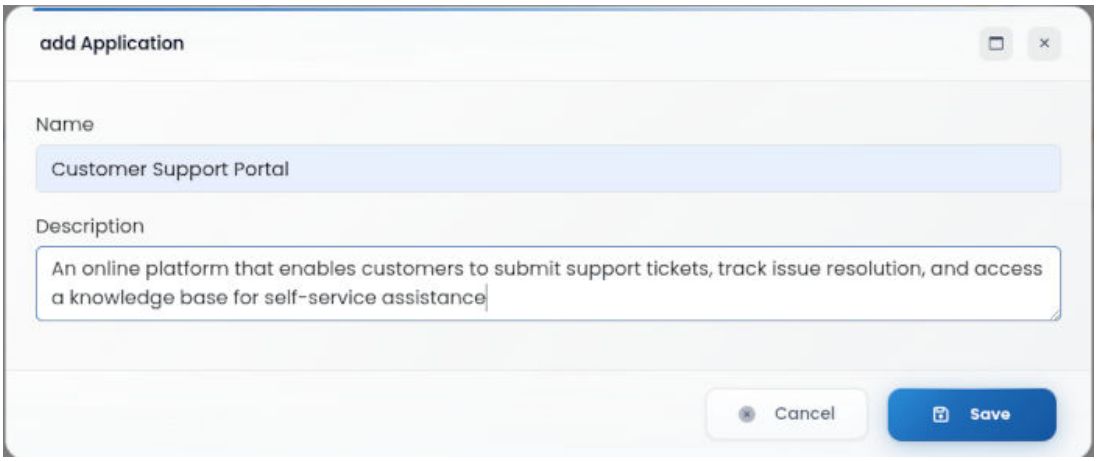
For instructions on adding a new asset, refer to the following link: How to ADD a New Asset

To see how to collect data on Active Directory Assets Information: How to collect data on Active Directory Assets Information

Applications

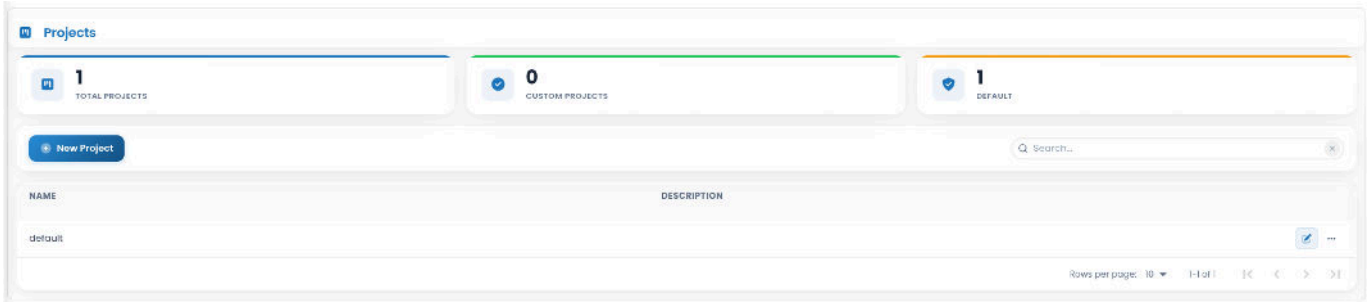
This section enables the configuration and management of applications within the system. Users can add new applications by entering a unique **Name** and providing a clear **Description** that outlines the application's purpose or functionality. These details help maintain organized records and facilitate easier identification and management of applications across the platform.

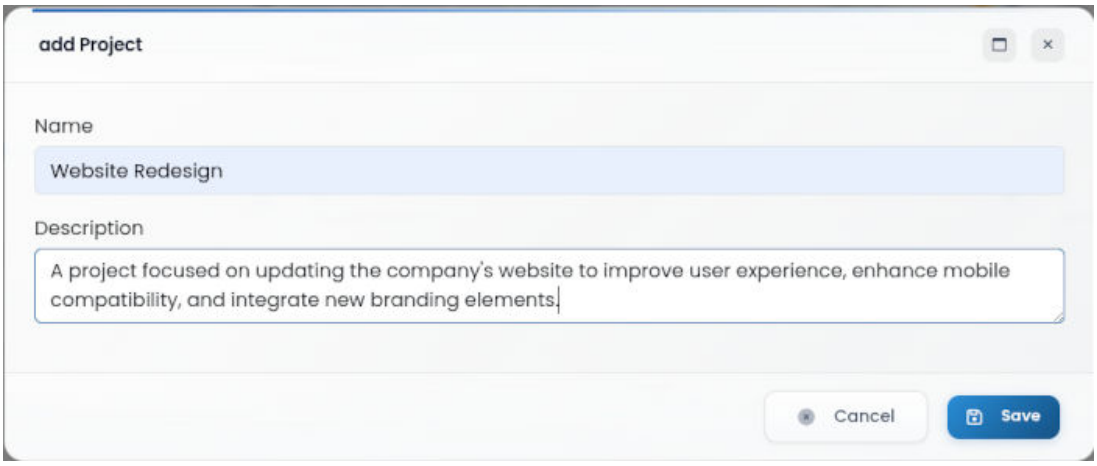




Projects

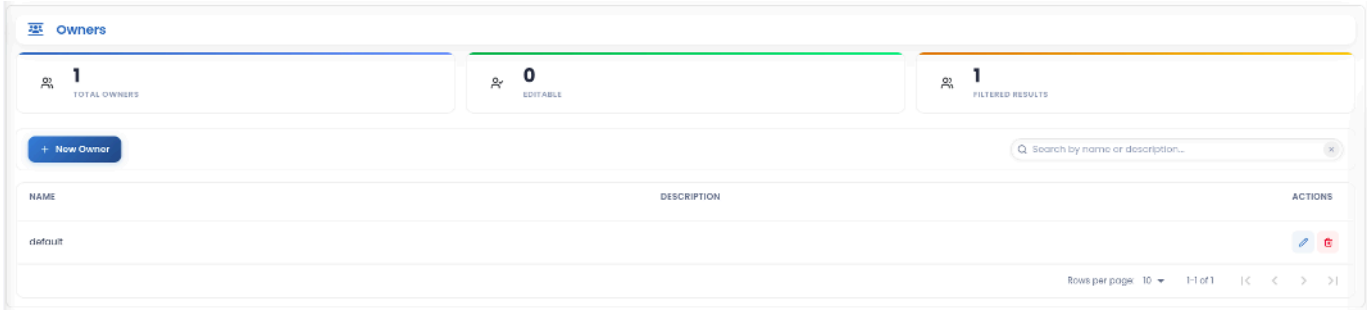
This section allows configuration and management of projects within the system. New projects can be created by specifying a **Name** and providing a detailed **Description** outlining the project's objectives, scope, or key activities.

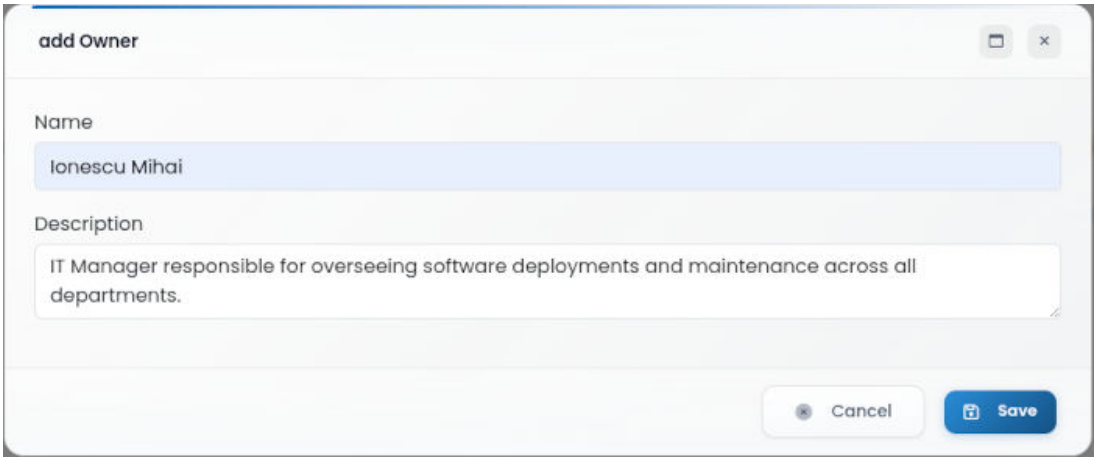




Owners

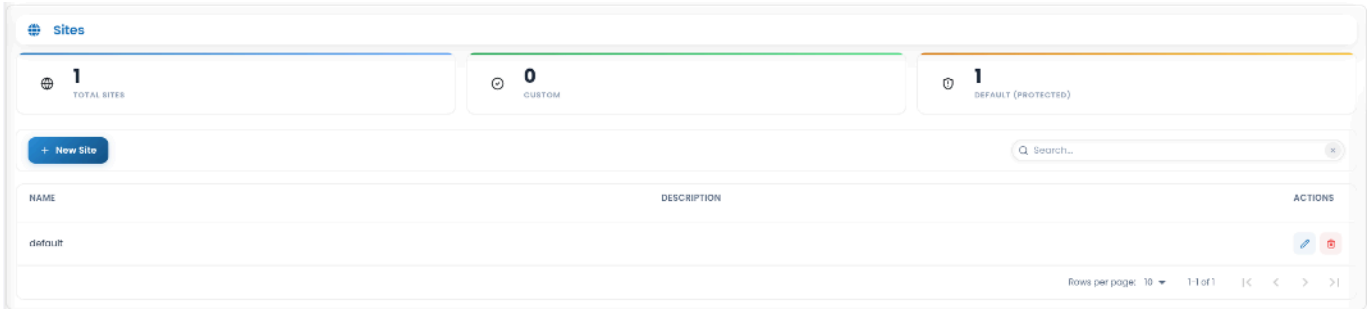
This section manages the configuration of owners responsible for assets, applications, or projects. New owners can be added by providing a **Name** and a brief **Description** that clarifies their role or area of responsibility.

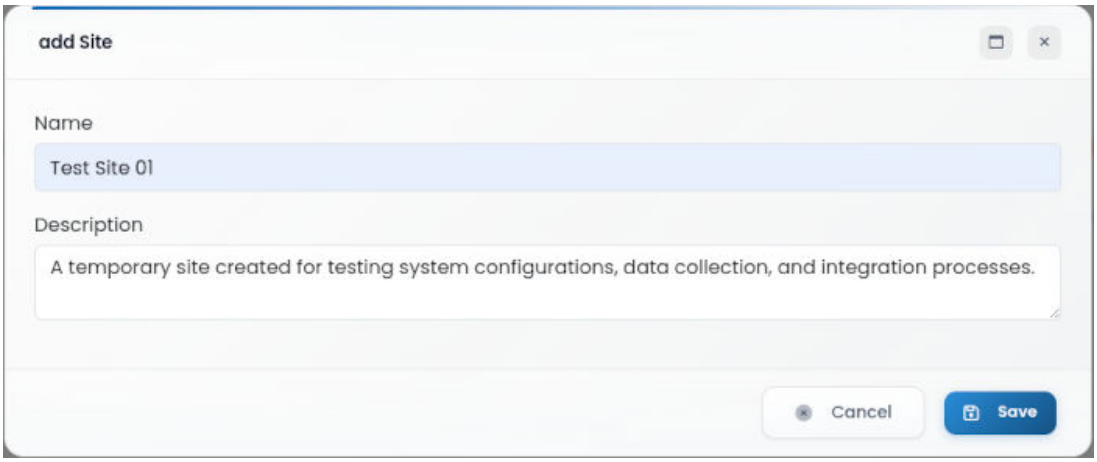




Sites

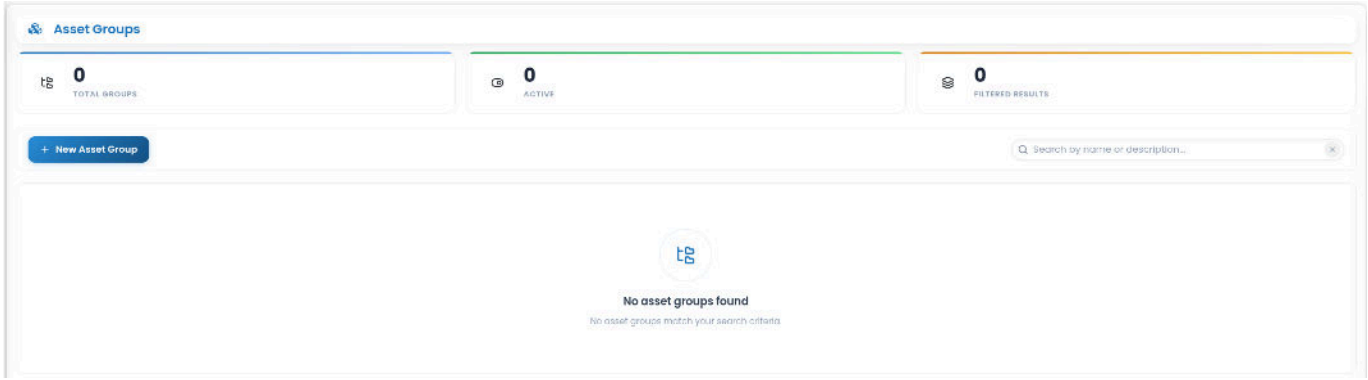
This section allows configuration and management of sites within the system. New sites can be created by entering a **Name** and providing a **Description** that outlines the site's purpose, location details, or operational scope.

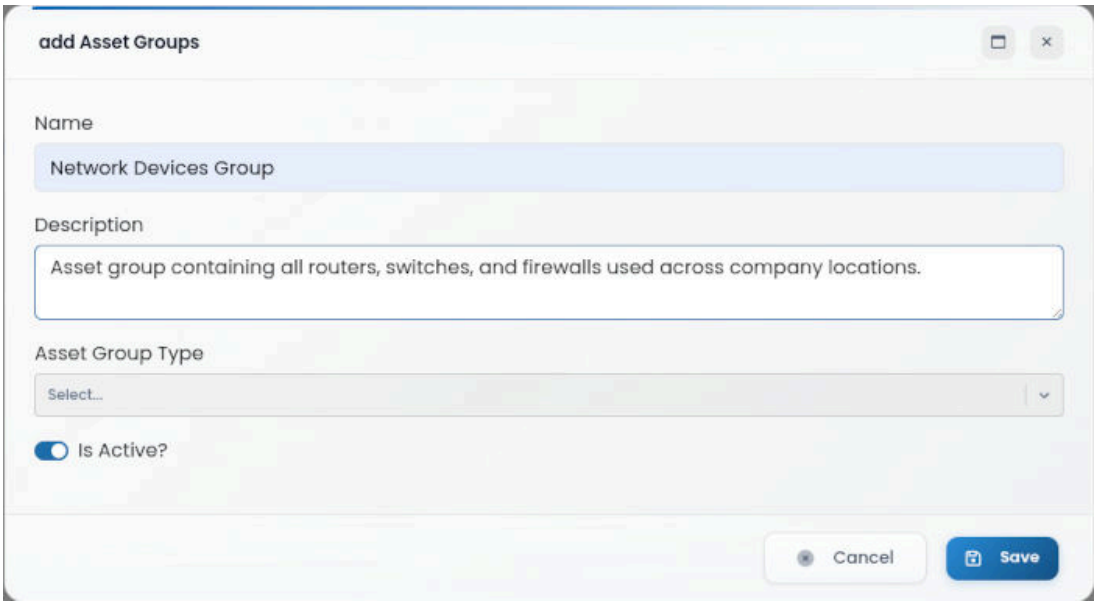




Asset groups

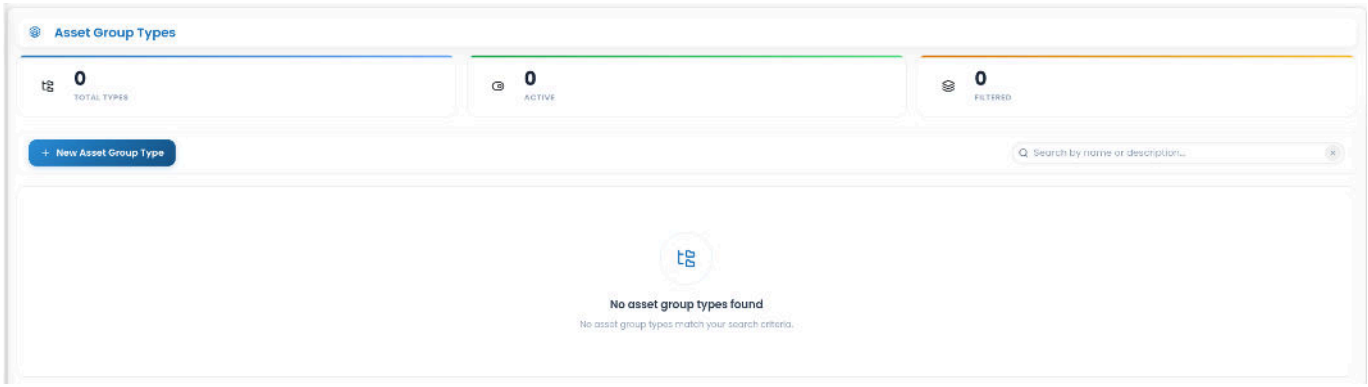
This page provides configuration options for asset groups. It allows assigning a specific asset group type to an existing asset group, ensuring proper organization and categorization of assets.





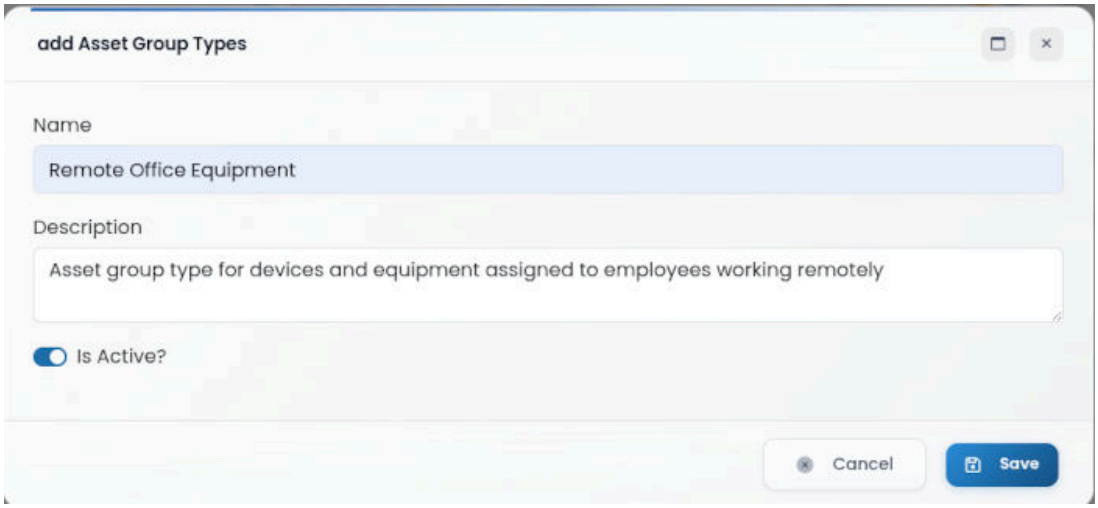
Asset Groups Types

This section is used for configuring asset group types, which define categories for organizing assets. All settings related to asset group types can be modified here to ensure accurate classification.



The **New Asset Group Type** screen includes the following fields:

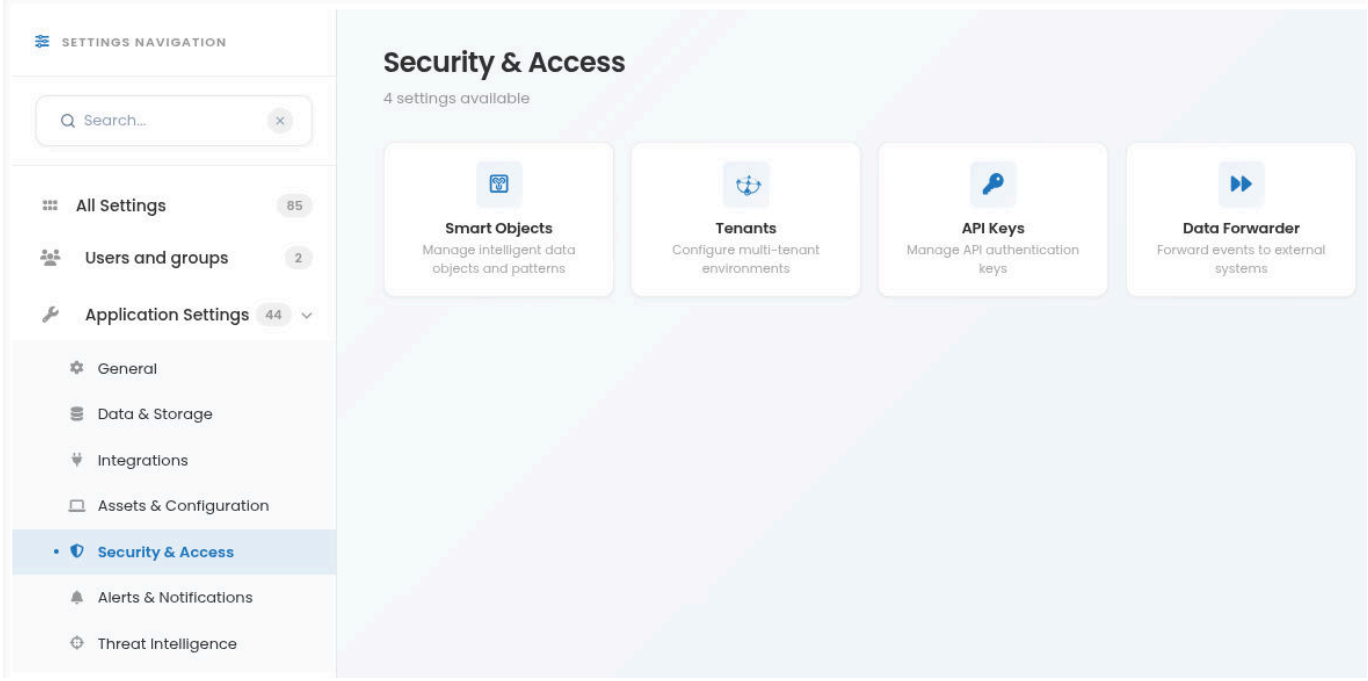
- Name - the name of the asset group type
- Description - a brief explanation of the asset group type
- Active / Disabled switch - used to enable or disable the asset group typ



Security & Access

The **Security & Access** section provides configuration areas related to access control, authentication, tenant management, API access, event forwarding, and intelligent data objects in CYBERQUEST.

To access this section, go to **Settings > Application Settings > Security & Access**.



The available options include:

- **Smart Objects** - Provides access to intelligent data object configuration used to enhance event analysis and investigation. Smart Objects can use information from one or more data streams to generate or enrich events. For detailed information, refer to the CYBERQUEST Smart Objects.
- **Tenants** - Configures tenant-related settings used to manage multi-tenant environments and tenant-specific platform behavior.
- **API Keys** - Manages API keys used to authenticate and control data access from external sources. Each key can define a name, authorized remote host, and active status.
- **Data Forwarder** - Configures event forwarding to external systems, such as a syslog server, and contains the parameters required for DataForwarder operation.

SmartObjects

The **Smart Objects** section allows administrators to enable or disable Smart Object settings used by CYBERQUEST during event processing and analysis. Smart Objects help enrich investigation context by generating or organizing events based on information collected from one or more data streams.

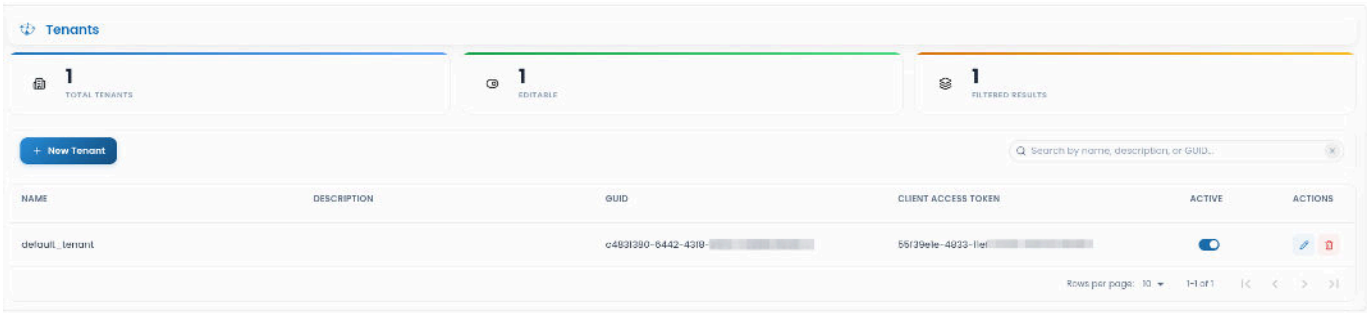
To access this section, go to **Settings > Application Settings > Security & Access > Smart Objects**.

The page displays the total number of Smart Object settings, including how many are currently **Active** or **Inactive**. Administrators can search for a specific Smart Object by name and use the **Active** toggle to enable or disable individual Smart Object settings.

For detailed configuration and usage information, refer to the CYBERQUEST Smart Objects.

Tenants

Select **Tenants** entry to change Tenants settings. Here you can change all entries that are related to Tenants.



API Keys

In the **API Keys** section, new entries can be created to control and authenticate data access from external sources. These settings define the name of the key, the authorized remote host, and whether the key is currently active.

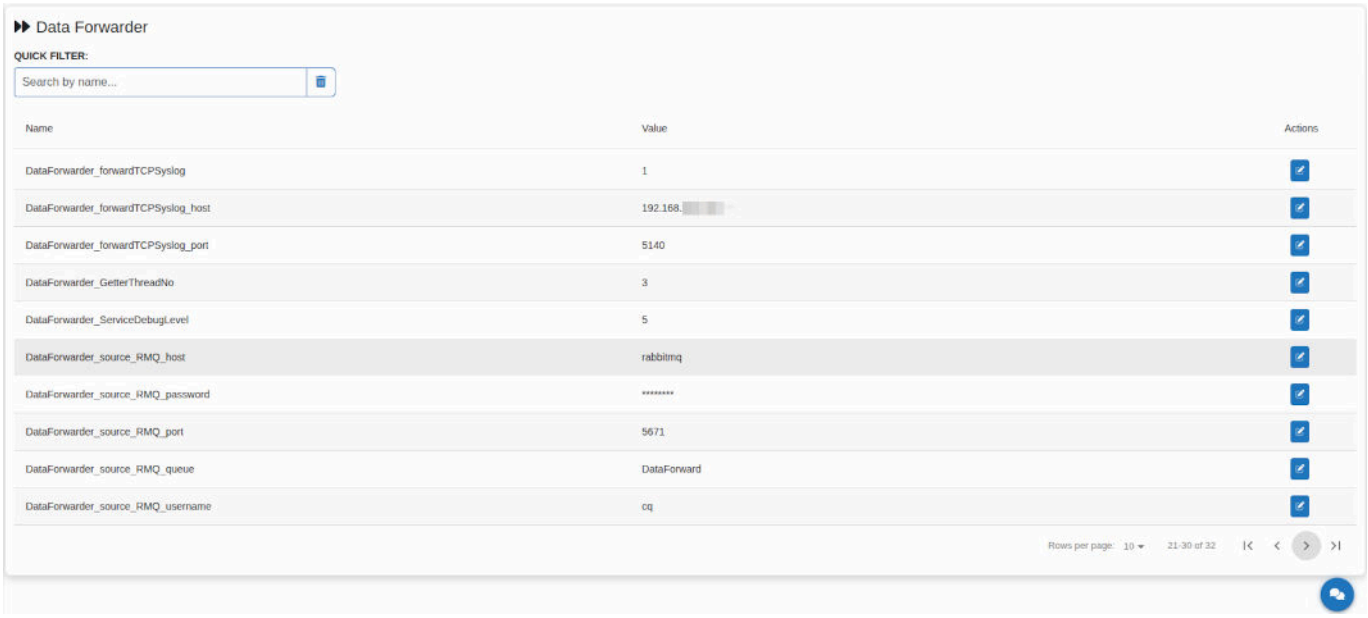




- **Name** - A descriptive label for the API key, used to identify its purpose or associated system.
- **Remote Host** - The IP address or hostname from which API requests are allowed.
- **Activate** - Enables or disables the API key

DataForwarder

Select **DataForwarder** to configure event forwarding to a syslog server. This section contains all parameters related to DataForwarder operation.



- **DataForwarder_cache_path** - Location where cache files are stored for temporarily holding events before forwarding
- **DataForwarder_enableForwarding** - Enables or disables the DataForwarder service (default is disabled)
- **DataForwarder_forwardCEF** - Enables forwarding of events in CEF (Common Event Format) - default is disabled

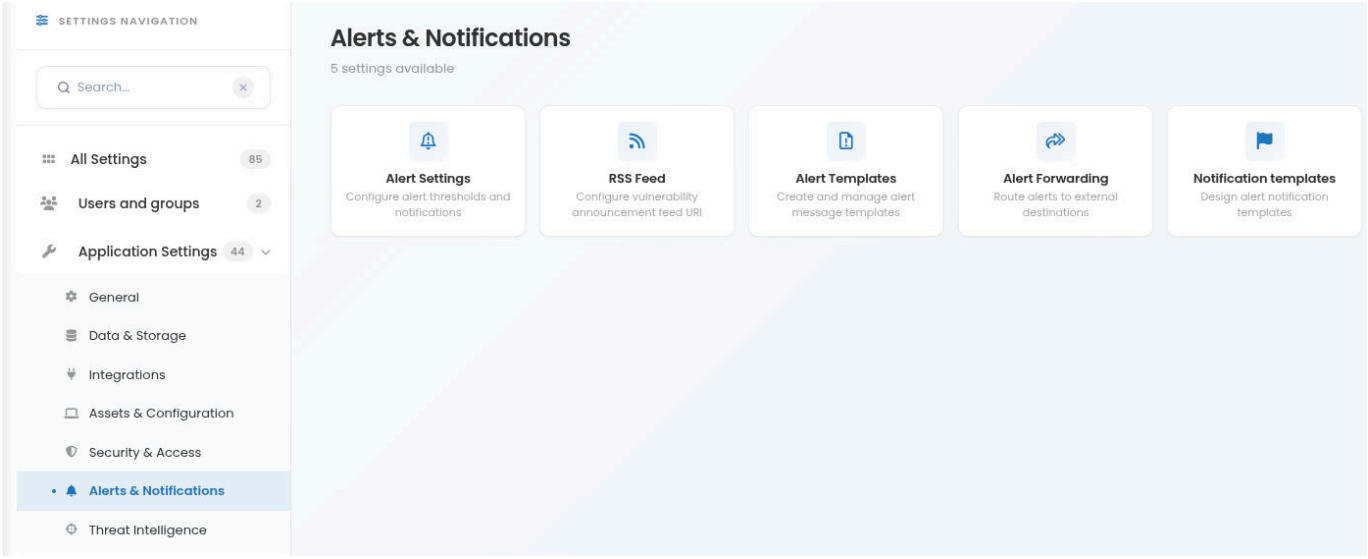
- **DataForwarder_forwardCEF_host** - Hostname or IP address of the CEF destination server
- **DataForwarder_forwardCEF_port** - Network port used for CEF event forwarding
- **DataForwarder_forwardCEF_protocol** - Network protocol used for CEF forwarding
- **DataForwarder_forwardLEEF** - Enables forwarding of events in LEEF (Log Event Extended Format) - default is disabled
- **DataForwarder_forwardLEEF_host** - Hostname or IP address of the LEEF destination server
- **DataForwarder_forwardLEEF_port** - Network port used for LEEF event forwarding
- **DataForwarder_forwardLEEF_protocol** - Network protocol used for LEEF forwarding
- **DataForwarder_forwardRMQ** - Enables event forwarding to another CYBERQUEST server via RabbitMQ
- **DataForwarder_forwardRMQ_host** - Hostname or IP address of the RabbitMQ server. In distributed architectures, this may differ from the default database server
- **DataForwarder_forwardRMQ_password** - Password used for RabbitMQ authentication
- **DataForwarder_forwardRMQ_port** - Network port used for RabbitMQ communication
- **DataForwarder_forwardRMQ_queue** - Name of the RabbitMQ queue used for forwarding events
- **DataForwarder_forwardRMQ_username** - Username for RabbitMQ authentication
- **DataForwarder_forwardSyslog** - Enables forwarding of events to a Syslog server (default is disabled)
- **DataForwarder_forwardSyslog_host** - Hostname or IP address of the Syslog server. In distributed architectures, this may differ from the default database server
- **DataForwarder_forwardSyslog_port** - Network port for Syslog forwarding
- **DataForwarder_forwardSyslog_protocol** - Network protocol for Syslog forwarding
- **DataForwarder_forwardTCPSyslog** - Enables forwarding of events to a Syslog server using TCP default is disabled)
- **DataForwarder_forwardTCPSyslog_host** - Hostname or IP address of the TCP Syslog server
- **DataForwarder_forwardTCPSyslog_port** - Network port for TCP Syslog forwarding
- **DataForwarder_GetterThreadNo** - Number of threads used to read events from the incoming queue
- **DataForwarder_ServiceDebugLevel** - Logging verbosity level: 0-FATAL ERROR, 1-WARNING, 2-INFO, 3-DEBUG
- **DataForwarder_source_RMQ_host** - Hostname or IP address of the RabbitMQ source server. In distributed architectures, this may differ from the default database server
- **DataForwarder_source_RMQ_password** - Password for authentication to the RabbitMQ source server
- **DataForwarder_source_RMQ_port** - Port used to connect to the RabbitMQ source server.
- **DataForwarder_source_RMQ_queue** - The messaging queue name for queuing services
- **DataForwarder_source_RMQ_username** - Username for authentication to the RabbitMQ source server
- **DataForwarder_throttle_queue** - Maximum number of events allowed in the message queue before forwarding stops. Additional events are cached locally until the queue clears
- **DataForwarder_UseDefaultParsers** - Specifies whether to use the internally defined parsers for all events

For additional details on DataForwarder, refer to: How to forward syslog data

Alerts & Notifications

The **Alerts & Notifications** section provides configuration areas for managing alert behavior, alert templates, forwarding rules, RSS feed settings, and notification templates in CYBERQUEST.

To access this section, go to **Settings > Application Settings > Alerts & Notifications**.

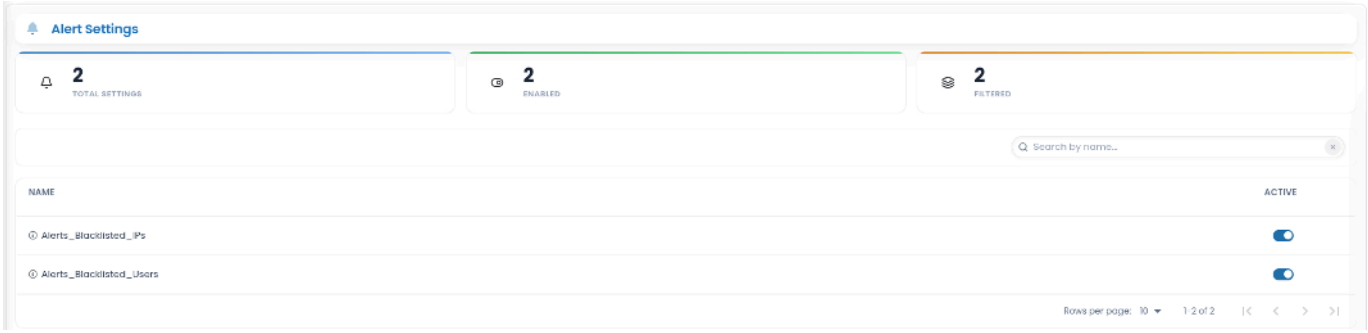


The available options include:

- **Alert Settings** - Configures alert-related parameters, including alert thresholds and notification behavior.
- **RSS Feed** - Configures the RSS feed URL used for vulnerability announcements or related security updates.
- **Alert Templates** - Manages the templates used to define alert message structure and content.
- **Alert Forwarding** - Configures alert forwarding to an external syslog server or other supported destinations.
- **Notification Templates** - Provides access to alert notification template customization. Templates can be created, edited, or deleted to control how alert notifications are presented. For detailed instructions, refer to the Notification templates customization.

Alert Settings

The **Alert Settings** section allows modification of all parameters related to alerts.



- Alerts_Blacklisted_IPs - it enables / disables the Blacklisted_IPs alert
- Alerts_Blacklisted_Users - it enables / disables the Blacklisted_Users alert

RSS Feed

The **RSS Feed** section allows administrators to configure the RSS feed URL used by CYBERQUEST to retrieve vulnerability announcements or security-related updates.

To access this section, go to **Settings > Application Settings > Alerts & Notifications > RSS Feed**.



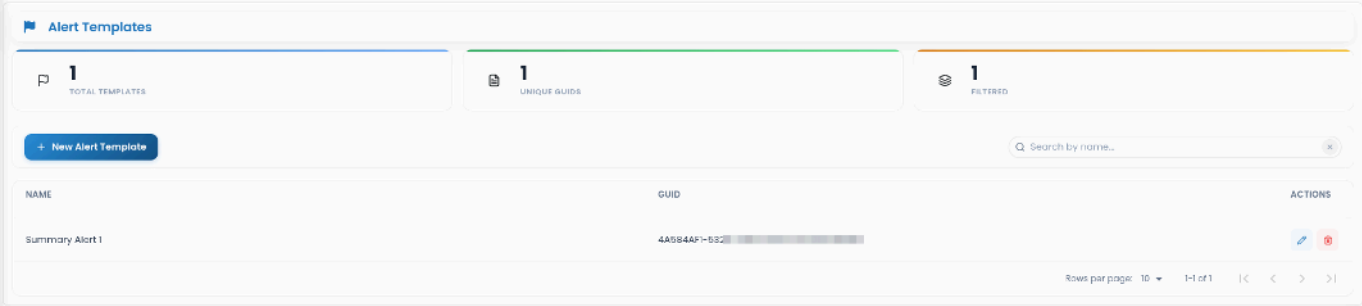
The page displays the configured RSS feed setting:

- **RSSFeedUri** - Defines the RSS feed URL used by CYBERQUEST to collect vulnerability or security announcement information.

To update the RSS feed URL, click the edit button from the **Actions** column, modify the value, and save the configuration.

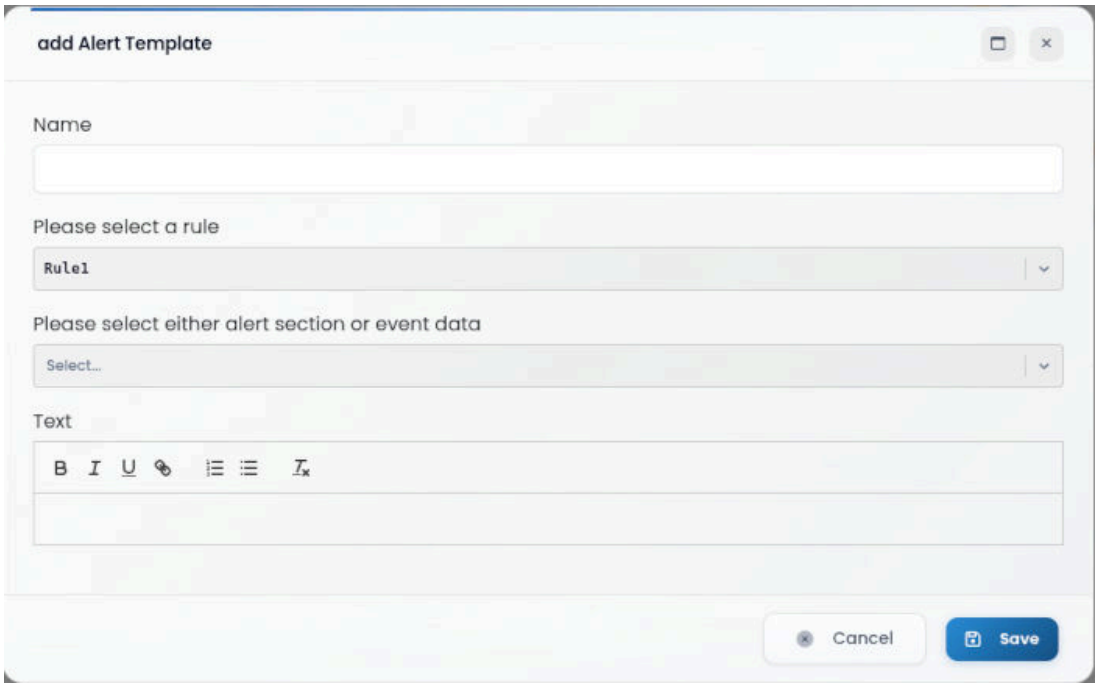
Alert Templates

The **Alert Templates** section allows configuration of all parameters related to alert templates.



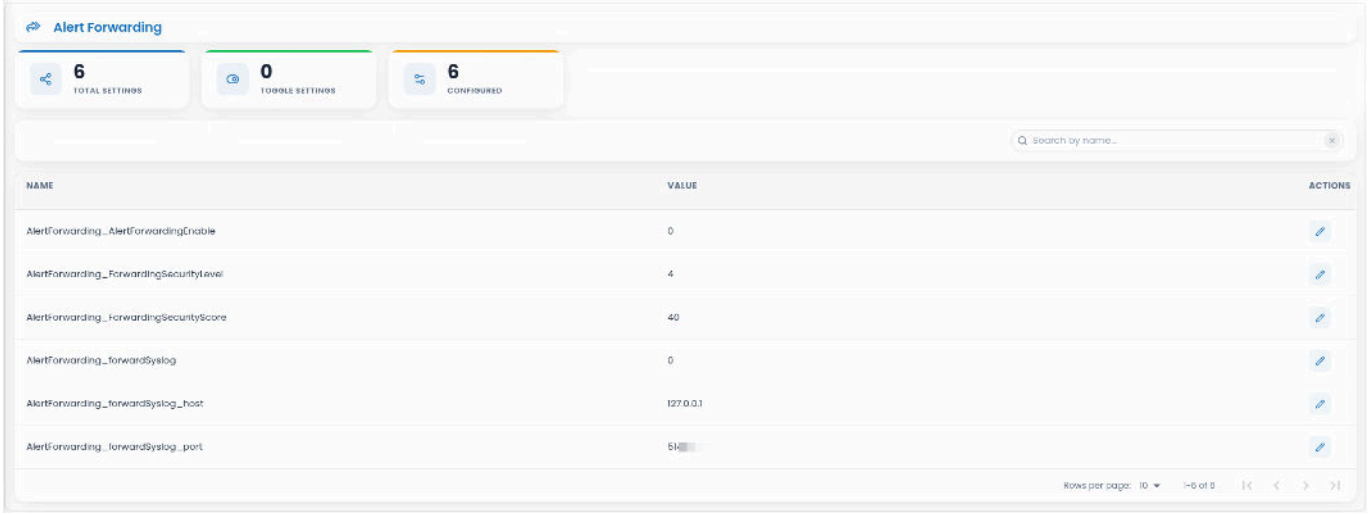
For creating a new alert template, please complete the following fields:

- **Name** - Enter a unique and descriptive name for the new alert template. This helps in easily identifying and managing the template later.
- From the **Please select a rule** drop-down list, choose the rule (e.g., *Rule1*, *Rule2*, *Rule3*, or *Rule4*) that the template will reference.
- In the **Please select either alert section or event data** field, specify whether to use an alert section or event data as the source.
- In the **Text** field, enter a descriptive message or insert dynamic objects as needed.



Alert Forwarding

Select the **Alert Forwarding** entry to configure alert forwarding to a syslog server. This section includes all parameters related to the Alert Forwarding process.



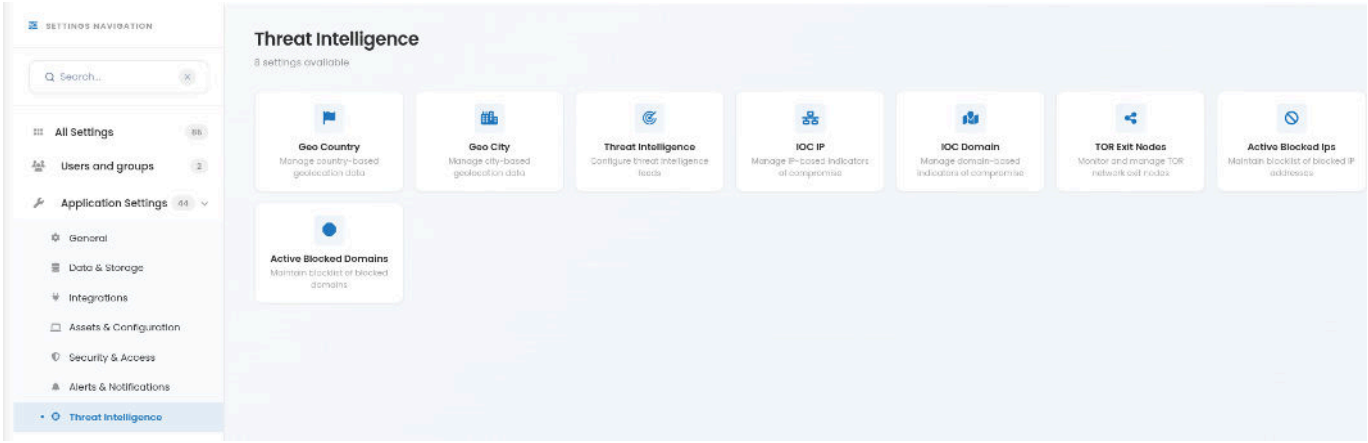
- AlertForwarding_AlertForwardingEnable - Enables or disables alert forwarding (default is disabled)
- AlertForwarding_ForwardingSecurityLevel - Defines the security level applied to forwarded alerts
- AlertForwarding_ForwardingSecurityScore - Defines the security score assigned to alerts during forwarding
- AlertForwarding_forwardSyslog - Enables Syslog-based alert forwarding (default is disabled)
- AlertForwarding_forwardSyslog_host - The host (IP or domain) to which Syslog alerts are forwarded
- AlertForwarding_forwardSyslog_port - The network port used for forwarding Syslog alerts

For additional details on AlertForwarding, refer to: How to forward alerts to another host

Threat Intelligence

The **Threat Intelligence** section provides access to configuration areas used to manage geolocation data, threat intelligence feeds, indicators of compromise, Tor exit nodes, and active blocklists in CYBERQUEST.

To access this section, go to **Settings > Application Settings > Threat Intelligence**.



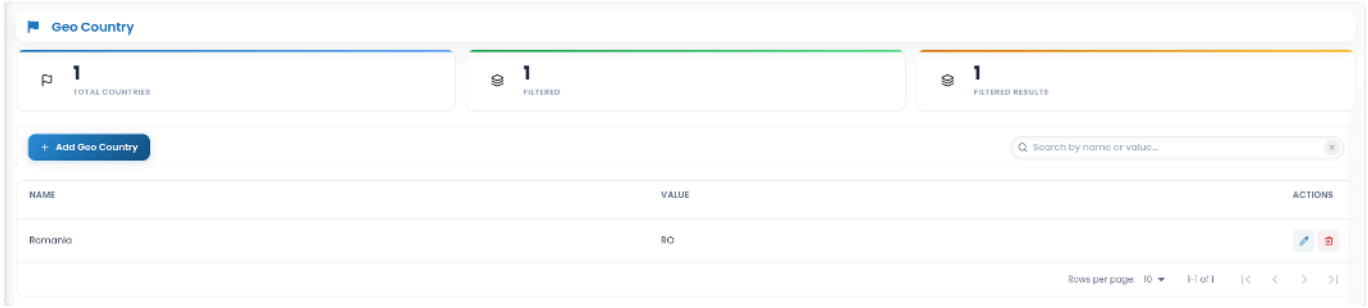
The available options include:

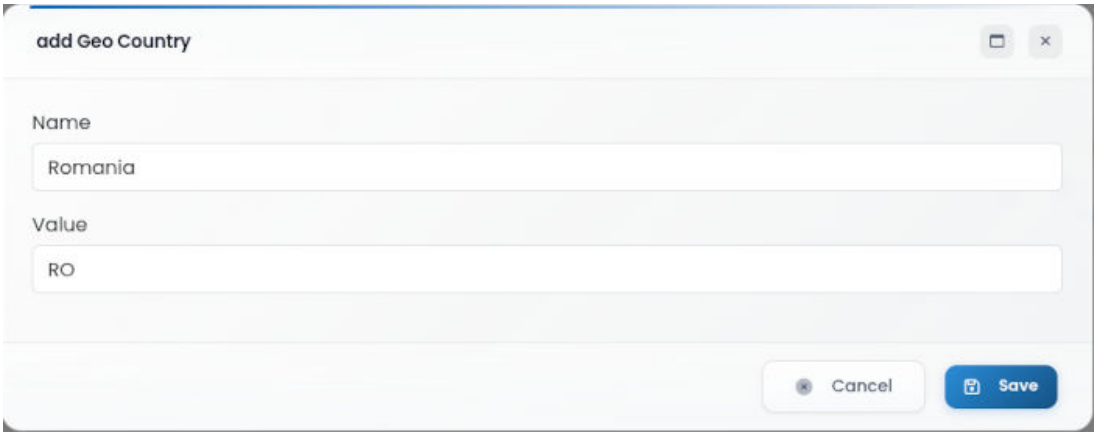
- **Geo Country** - Manages country-based geolocation entries used by CYBERQUEST for enrichment, filtering, and reporting.
- **Geo City** - Manages city-based geolocation entries used to provide more detailed location context for IP-related events.
- **Threat Intelligence** - Provides access to threat intelligence feed configuration and management. For detailed information, refer to the Threat Intelligence.
- **IOC IP** - Manages IP-based indicators of compromise used for detection, correlation, and investigation.
- **IOC Domain** - Manages domain-based indicators of compromise used to detect or correlate activity involving suspicious or malicious domains.
- **TOR Exit Nodes** - Manages known Tor exit node entries used for detection, filtering, or monitoring of Tor-related network activity.
- **Active Blocked IPs** - Manages IP addresses currently blocked by the system, including details such as expiration time, block list association, and comments.

- **Active Blocked Domains** - Manages domains currently blocked by the system, allowing administrators to maintain and review restricted domain entries.

Geo Country

Select **Geo Country** to manage geographic country entries used by the system. This section allows adding new countries and configuring their associated values.

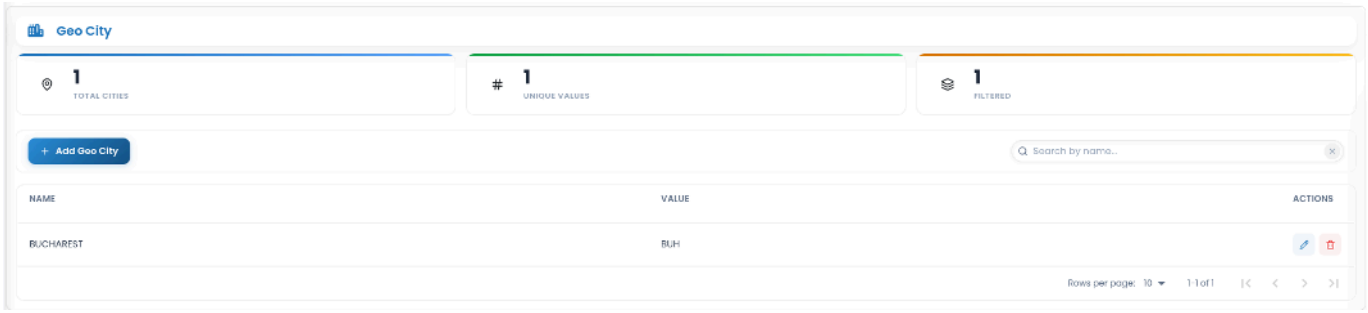




- **Name** - The official name of the country
- **Value** - The system-assigned code or identifier associated with the country

Geo City

Select **Geo City** to manage geographic city entries used by the system. This section allows adding new cities and configuring their associated values.

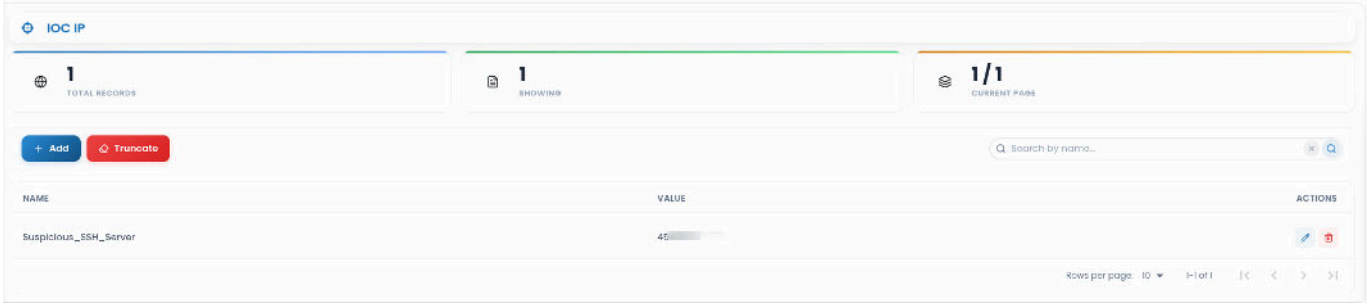




- **Name:** The name of the city (*e.g., Bucharest*)
- **Value:** A unique identifier or code for the city (*e.g., BUH*)

IOC IP

Select **IOC IP** to manage IP indicators of compromise used by the system. This section allows adding new IP entries and configuring their associated values.



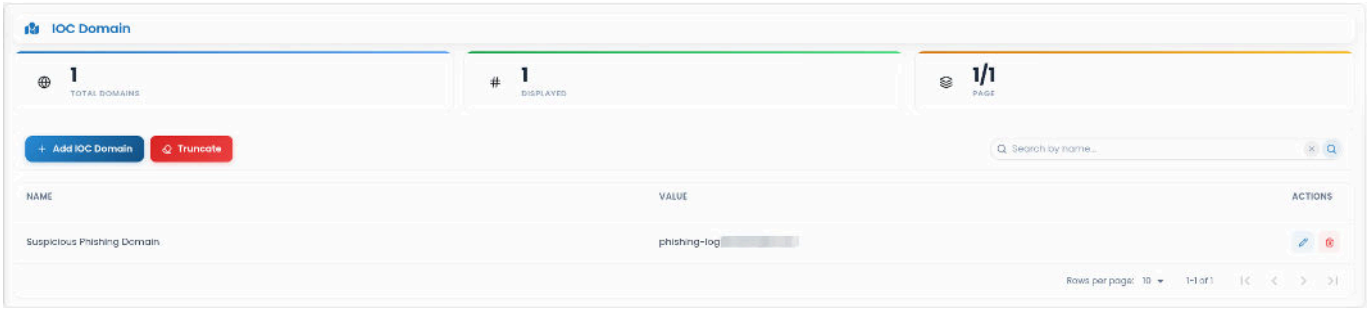


- **Name** - The descriptive name of the IP entry
- **Value** - The IP address associated with the entry

Truncate button - Clears all entries in the current IOC IP list, removing all stored IP addresses.

IOC Domain

Select **IOC Domain** to manage domain-based Indicators of Compromise (IOCs) used by the system for threat detection and correlation. This section allows adding new domains and configuring their associated values.





- **Name** - A descriptive label for the IOC domain entry, helping identify its purpose or source
- **Value** - The specific domain name associated with the IOC entry (e.g., `maliciousdomain.com`)

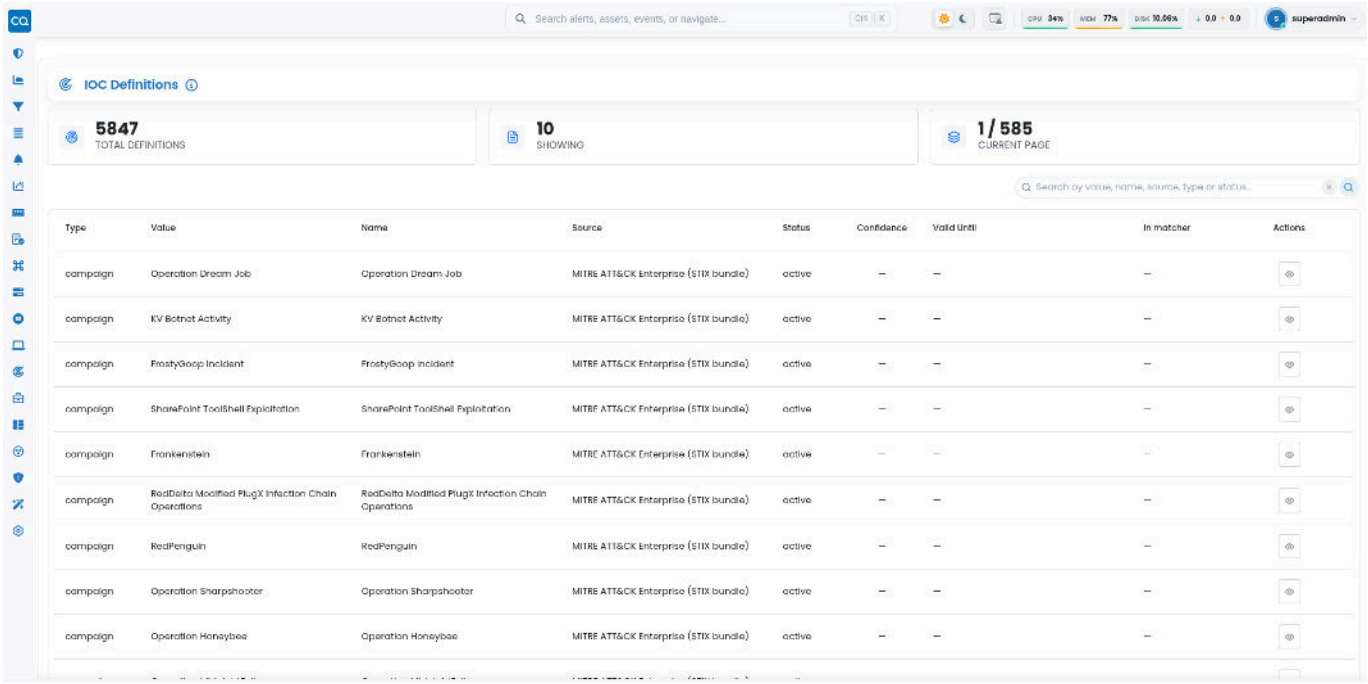
Truncate button - Deletes all existing IOC Domain entries from the list, clearing the stored data entirely. This action cannot be undone.

IOC Definitions

The **IOC Definitions** page provides a centralized view of the threat intelligence definitions and STIX objects imported or synchronized from configured **Threat Intelligence** sources.

For information about configuring, importing, and synchronizing Threat Intelligence sources, see Threat Intelligence.

To access the page, navigate to **Settings > Application Settings > IOC Definitions**:



The following information is available for each definition:

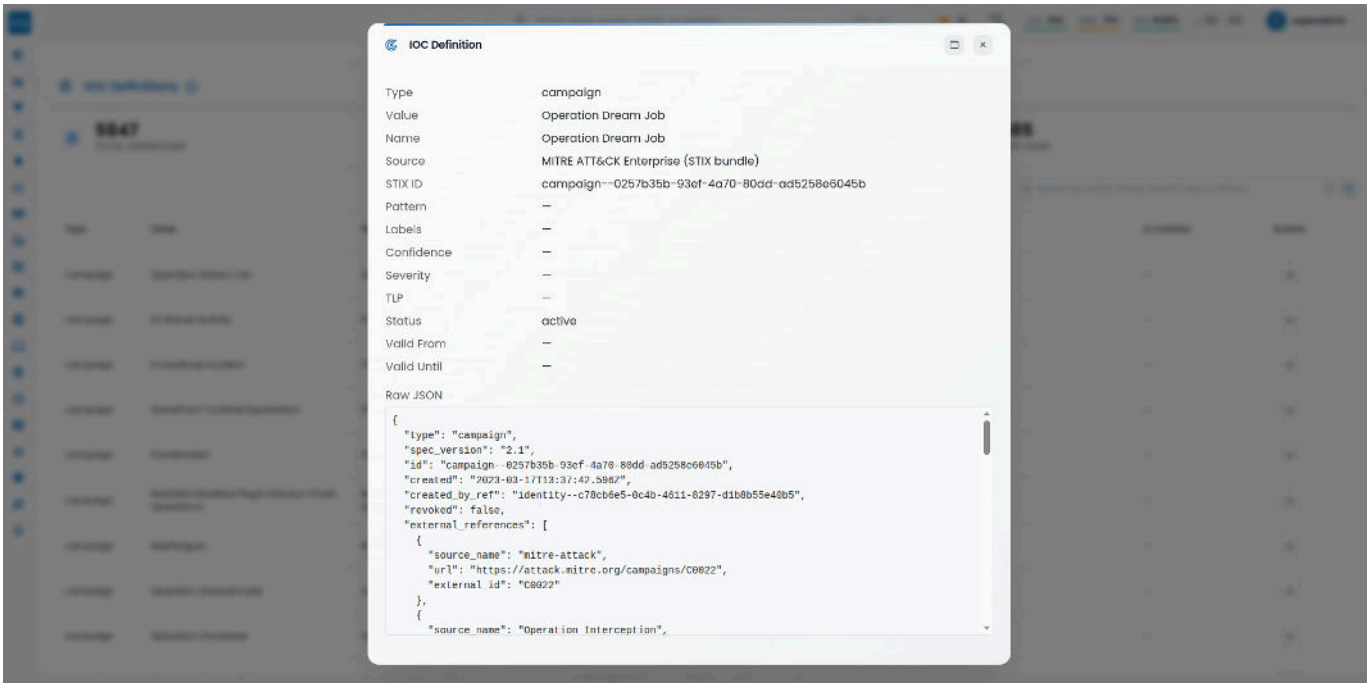
- **Type** - Identifies the type of the imported definition or STIX object, such as `indicator`, `campaign`, or other supported object types.
- **Value** - Displays the value associated with the definition.
- **Name** - Displays the human-readable name of the definition.
- **Source** - Identifies the Threat Intelligence source from which the definition was imported or synchronized.
- **Status** - Shows the current status of the definition.
- **Confidence** - Displays the confidence value supplied by the source, when available.
- **Valid Until** - Shows the expiration date of the definition, when provided by the source.
- **In matcher** - Indicates whether the definition is available to the matching mechanism.
- **Actions** - Provides access to the detailed information associated with the selected definition.

The search field can be used to locate definitions by **value, name, source, type, or status**.

Viewing an IOC Definition

Click the **View** action for a definition to open its detailed information.

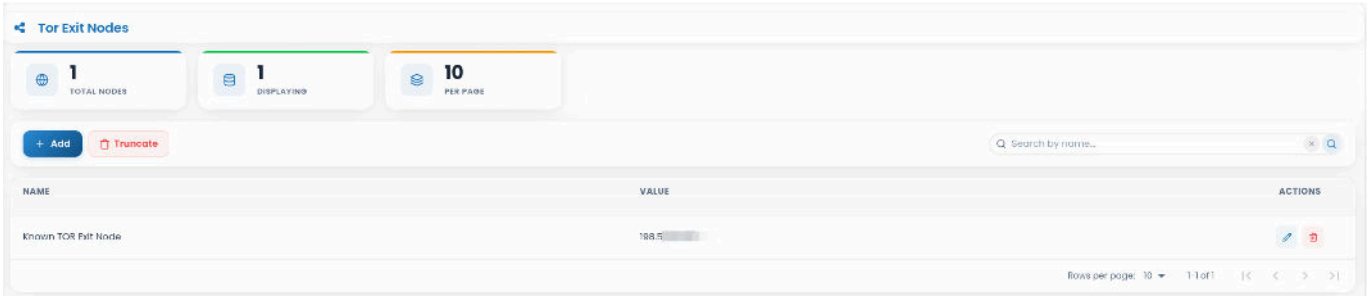
Depending on the imported STIX object, the following information may be available:

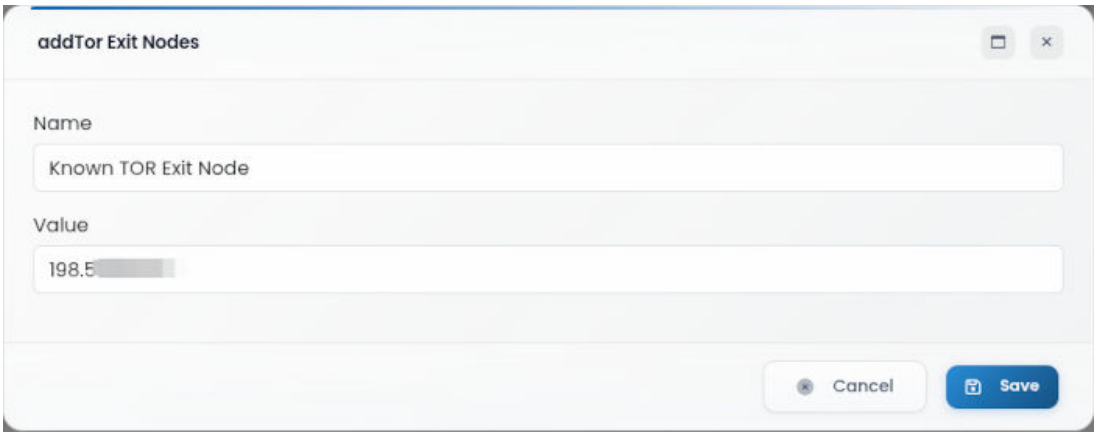


The **Raw JSON** section displays the original STIX object associated with the definition, preserving the source data and providing additional context for analysis and traceability.

Tor Exit Nodes

Select **Tor Exit Nodes** to manage a list of known Tor network exit nodes used by the system for detection or filtering purposes. This section allows adding new entries and assigning values to them.



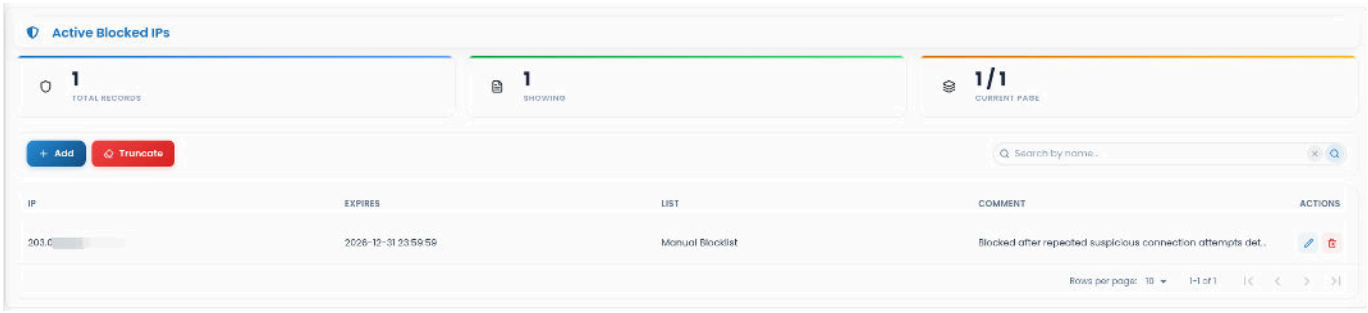


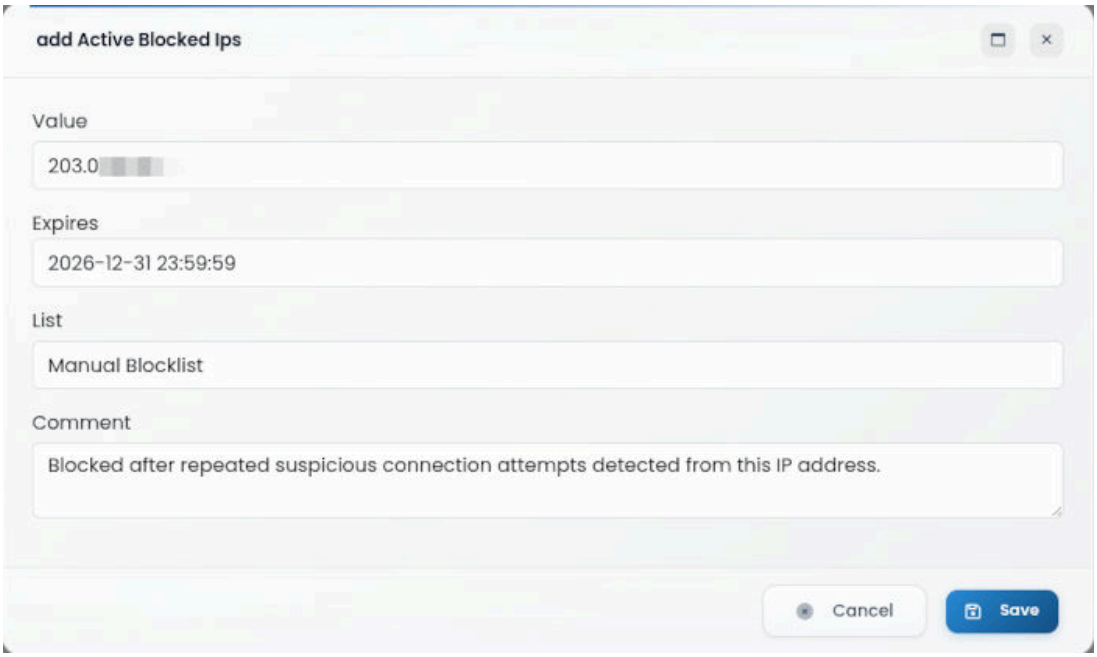
- **Name** - The label or identifier for the Tor Exit Node entry
- **Value** - The IP address of the Tor Exit Node

Truncate button - Permanently clears all stored Tor Exit Node entries from the list, removing both names and values

Active Blocked Ips

The **Active Blocked IPs** section is used to manage IP addresses that are currently blocked by the system. New entries can be added, along with details such as expiration time, associated block list, and comments for reference. This helps maintain control over restricted IP addresses and provides context for each block.

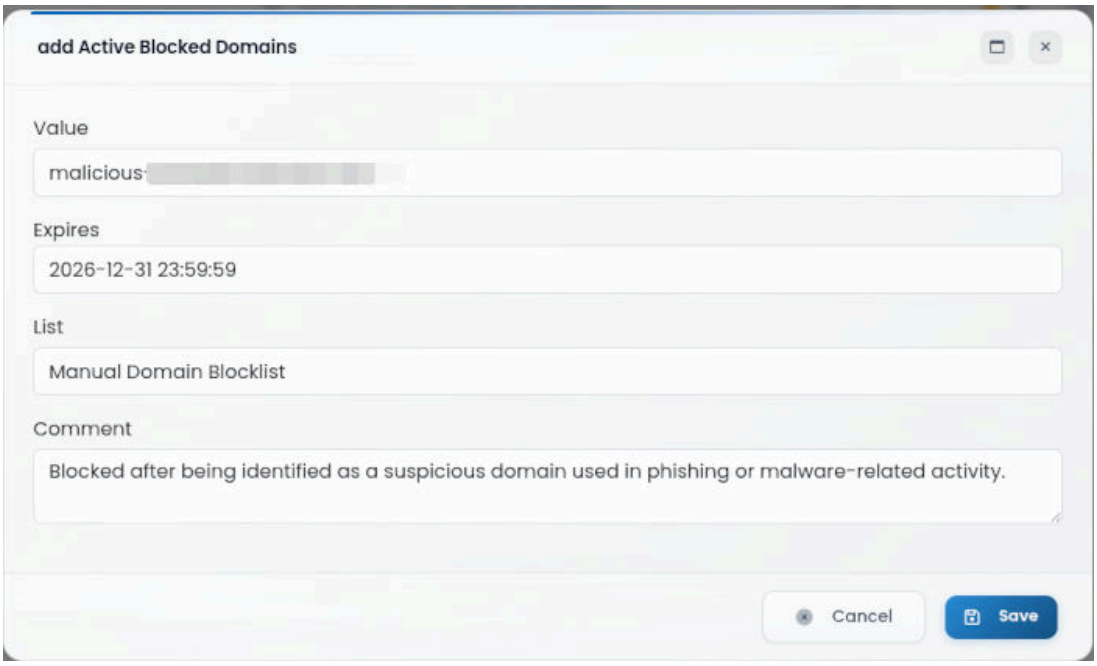




Active Blocked Domains

Active Blocked Domains - Manages domains that are currently blocked by CYBERQUEST. Each entry can include the blocked domain, expiration date, blocklist name, and a comment explaining why the domain was blocked.





Alerts

How to create new alerts

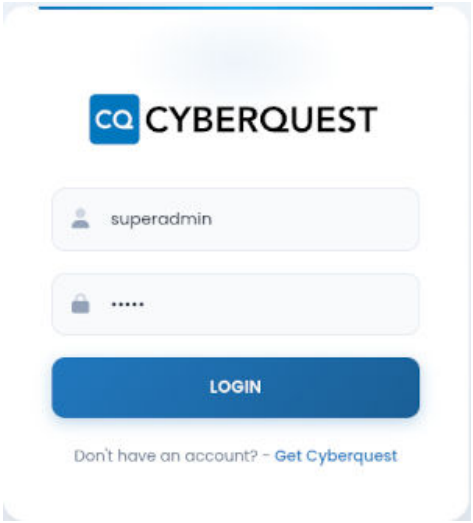
CYBERQUEST's alerting feature is a completely customizable module for each connected user. The event triggering an alert can be user-defined to respond to specific event needs, ensuring great accuracy and reducing false alerting to a minimum.

Follow the steps to create a new alert:

Step 1. Authentication

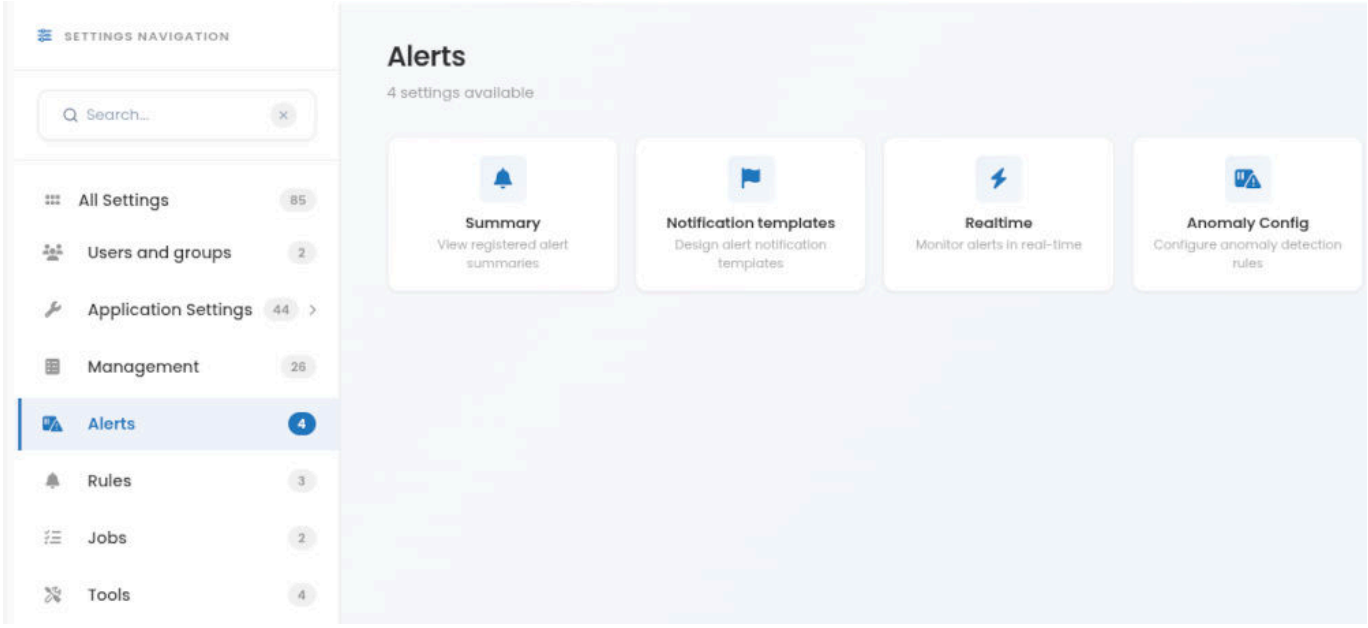
To access Web Interface, open a web browser and type the application's address or DNS name. The default address initially assigned to Web Interface is ***https://CyberquestIPAddress*** (example).

The browser automatically redirects you to CYBERQUEST's authentication page:



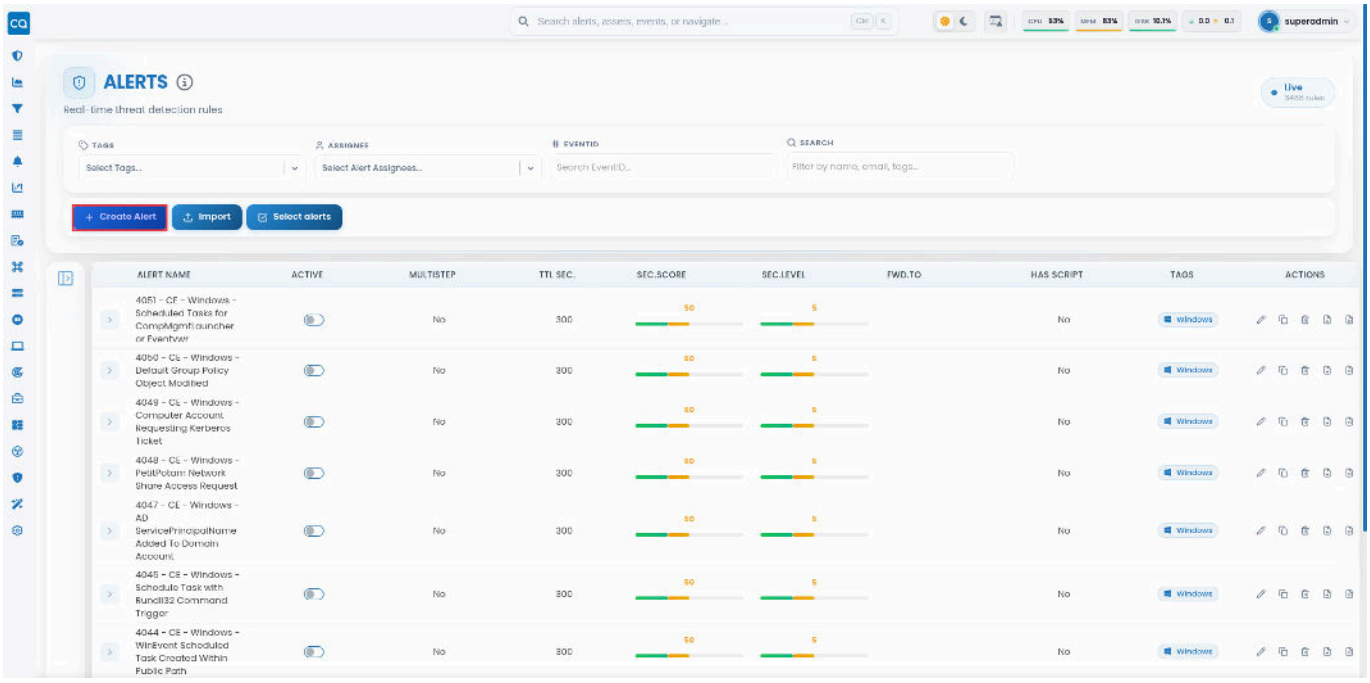
Step 2. Navigate to Alerts

From **Settings** menu, select **Alerts > Realtime**. **Alerts** customization page opens in **Alerts** module interface.



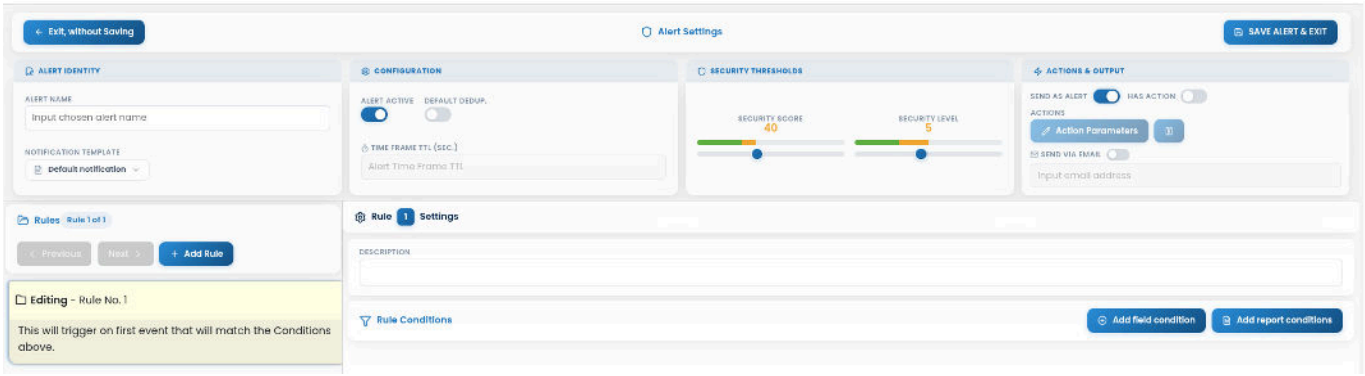
Step 3. Create new alert definition

On the “Alerts” page, select the “CREATE ALERT” button to create a new alert.



Step 4. Complete the form

Complete the form with the appropriate information and press “Save Alert & Exit” button:



Alert Name: The name of the new alert.

Alert Active: Select **ALERT ACTIVE** checkbox if the alert is active or uncheck to deactivate it.

Time Frame TTL(sec.) : This setting instructs the alert for how long to be active once triggered.

Alert Security Score: Defines the baseline security score (0-100) for the alert. When triggered, the score dynamically increases based on matching events and rule conditions, but cannot fall below this baseline or exceed 100. For example, a baseline of 70 with a rule that adds +5 per matching event would result in scores between 70-100. This score directly determines the alert’s severity level (see Security Level section).

Alert Security Level: Maps directly to the security score range (0-30: Low, 31-70: Medium, 71-100: High) with corresponding color coding (Green, Yellow, Red). This determines the visual representation in dashboards and notifications.

Sent as Alert: Send as Alert checkbox has a similar effect to **ALERT ACTIVE** checkbox. When unchecked, the alert is active but will not produce any visible effect. This setting ensures backend correlation of anomaly analysis over multiple events, triggers and alerts.

Has Action: If a script execution can be associated with the alert, check also **Has Action** checkbox. Script rule is the last rule in rule conditions list and prevails all other rules. Press “Action Parameters” button to open Script Editor window where you can create a custom script to apply as rule.

Send via Email: Send via Email checkbox allows the alert being sent to defined recipients.

Notification Template: Choose a notification template to apply to your alert. You can choose from built-in or custom notification templates. Default is Default notification.

Under Rules section, you can granularly define rules controlling the alert behaviour. You can define from single event rules to any correlation between events, order in which events occur, correlation to missing an event from a logical succession of events and so on.

Previous: Navigate through the condition of an alert.

Next: Navigate through the condition of an alert.

Add Rule: Add a new rule by pressing "Add Rule" button. The new rule is defined in Rule Settings pane to the right.

Rule Settings pane assists in defining the rule logic. Rule logic consists of field, report, and correlation conditions separated by logical operators AND, OR, and NOT. For example, to detect multiple failed logins: `(EventID = 4625 AND Status = "Failure") OR (EventID = 4649 AND Substatus = "0xC000006D")` within a 5-minute window.

Each rule has:

Description: A Description where you enter a text describing the rule.

Add field condition: In Select Field drop-down, select a representative event field. From the next drop-down select the appropriate value operator. In the third field enter desired value.

Add report condition: The rule condition presents you with a drop-down list from which you can select a report from all existing reports.

Delete: You can delete a rule condition.

When adding a rule condition, a logical operator is automatically added for correlation to the previous condition. The default operator is AND. Click on **AND** switch to change the logical value to **OR**. Click again to change back to AND.

If logical chain requires, a "NOT" operator is also added in the form of a checkbox. By default, the operator is not selected. Click **NOT** to select the operator.

To check additional information about **ALERTS**, please follow the link: Alerts Module.

Data flow rules and filters

Introduction to DTS

CYBERQUEST's Data Transformation Services (DTS) processes raw event data through custom JavaScript transformations, extracting meaningful fields from unstructured logs. For instance, it can split combined log entries into distinct user identifiers, timestamps, and action types for analysis.

Data Transformation Services extends and expands native CYBERQUEST capabilities with custom logic to further enrich and complete use cases:

- can help prepare data for future easy access, allowing data to be transformed and loaded from heterogeneous sources;
- can be used for event data correlation;
- adds, modifies, removes, enriches and obfuscates partial or complete event data;
- can remove an event;
- dynamically creates and fulfills default set up lists with data collected from incoming events (for example, a list of Blacklist IPs). Built in lists can be modified/added in Object Manager;
- can extract information from previously defined lists and take specific actions, such as sending alerts;

- uses a built-in JavaScript engine, the administrator being able to engage out-of-the-box or create custom logic for performing various actions;
- can send alerts;
- encrypts and decrypts data;
- can send HTTP/HTTPS requests for external systems/APIs;
- can query data stored in events database;
- and more.
- DTS Service stores in memory lists of objects that the user can use to do specific tasks. For example, **User logged on from specified IP ADDRESS** list can be accessed by using the following script:

```
if(Event.UserName == 'undefined')
{
    Event.UserName = CQ.Utils.LocalStorage.get('UserLists',Event.SrcIP);
}
```

Generic Lists

```
if(Event.EventType == 'undefined')
{
    Event.EventType = CQ.Utils.LocalStorage.get('list_name', Event.PropertyName);
}
```

Custom lists with dynamic objects can be created, which are shared between all components. The lists can be populated directly from DTS by using the "set" method from **LocalStorage** object. To achieve this, use the following method:

```
if(Event.EventType == '16') // 16 means Failed Audit event
{
    CQ.Utils.LocalStorage.set('hosts_with_failed_audit', Event.Computer, Event.Computer);
}
```

LocalStorage object exposes several methods of interacting with user lists

set() Method

Example:

```
CQ.Utils.LocalStorage.set(listName, objectName, objectValue, 900)
```

Description: This method stores user defined data into internal object lists which can also be edited in the Object Manager.

Parameters:

listName defines the list on which we operate. This parameter is required.

objectName defines the object name which is used for setting/retrieving data. This parameter is required.

objectValue The value to store (required). This parameter is optional. When it is not specified, the system will automatically use a **ttl** (Time-to-live) in seconds (default: 900; use -1 for indefinite storage).

get() Method

Example:

```
CQ.Utils.LocalStorage.get(listName, objectName)
```

Description: This method retrives user defined data from internal object lists which can also be edited in the Object Manager.

Parameters:

listName defines the list on which we operate. This parameter is required.

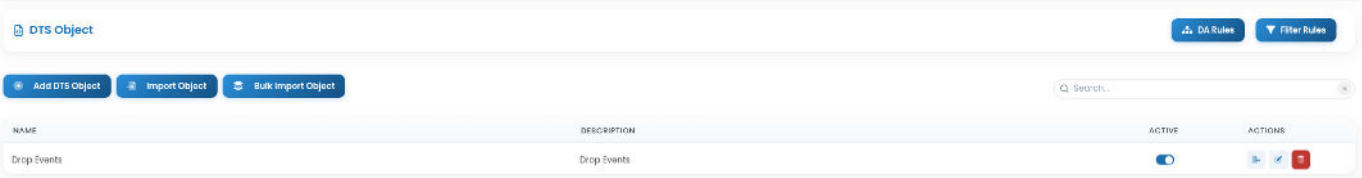
objectName defines the object name which is used for setting/retrieving data. This parameter is required.

JS parsers (DTS objects)

Parsing or syntactic analysis is the process of analyzing a string of symbols, either in natural language or in computer languages, conforming to rules of a formal grammar. The parser's task is essential to determine if and how the input can be derived from grammar's start symbol.

JS Parser is a Javascript object that uses event logs and intelligently sorts data, making it easier for a user to interpret resulted information. Parsing is done by calling ***obj.exec*** with the event as a parameter in JSON Format.

JavaScript (JS) parsers can be managed through the Web Interface under **Settings > Rules > DTS Objects**. The **DTS Objects** page displays all defined objects and provides options to import an existing object or create a new one from scratch. The **Actions** menu allows editing, deleting, or exporting a parser, as well as enabling or disabling it.



- To export a parser, press

  button next to it. The export is saved as a proprietary CQO file. Likewise, to import a parser select

  in **DTS Objects** page.

- To edit details for a specific object, press

  button next to it. **Edit DTS Objects** page opens allowing you to change the Name and Description, the Script or active/inactive the object.

- To delete a parser from the list, press

  button next to it. As a measure of precaution, you will be asked to confirm deletion.

- To mark a parser as activate/inactivate, press

  button.

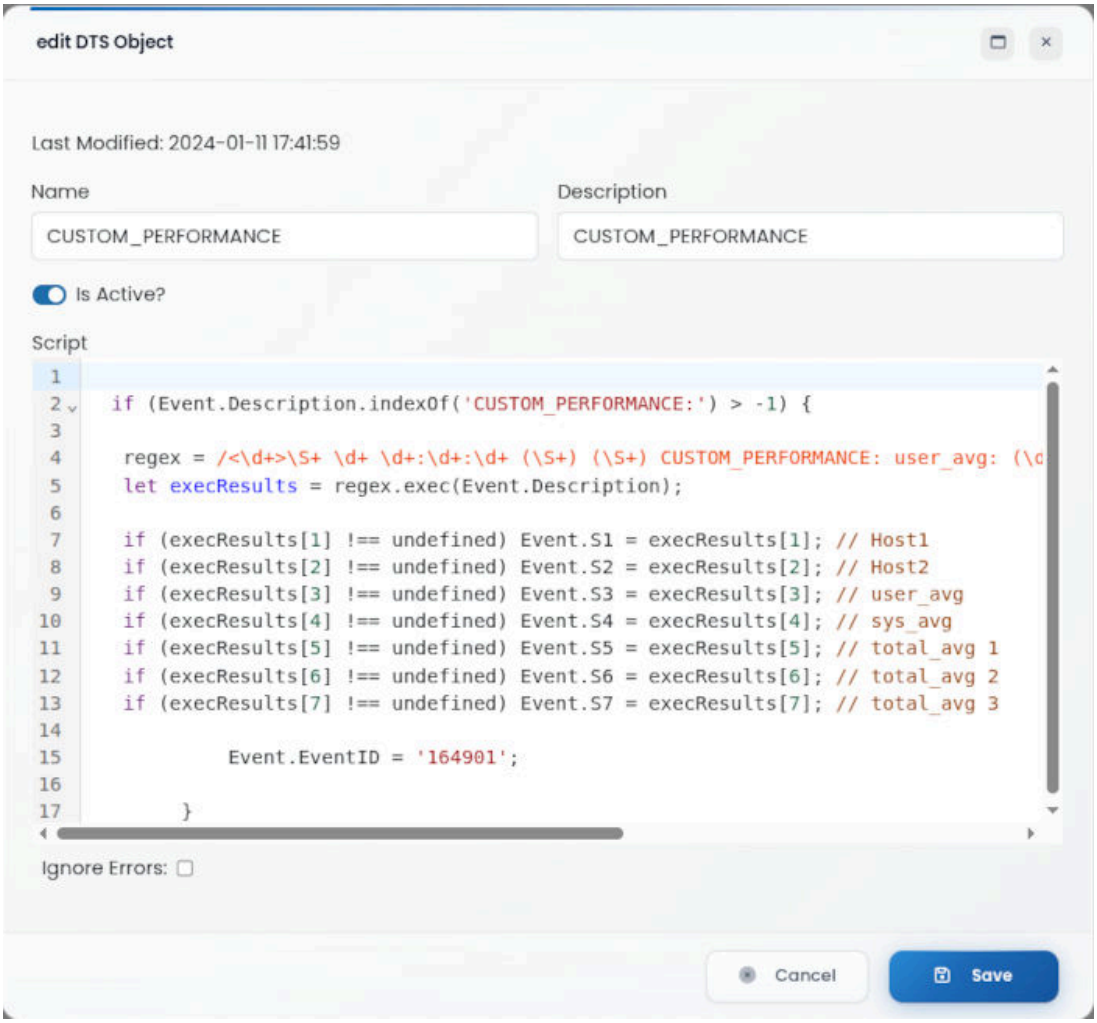
- Creating a new JS parser.

In **DTS Objects** page, select

Add DTS Object

button and configuration page opens allowing you to create the script for a new parser and mark it as active or inactive. When you finished creating the parser, press “Save” button to save changes.

Here is a sample JS parser:



Complete the following fields:

- In **Name** field, type a name that identifies the newly created DTS Object
- In **Description** field, insert a description of the object
- Use the field **is Active** to activate/inactivate the object
- In **Script** field, add the javascript code

When you finished creating the parser, press “Save” button to save changes or press “Cancel” button to discard changes.

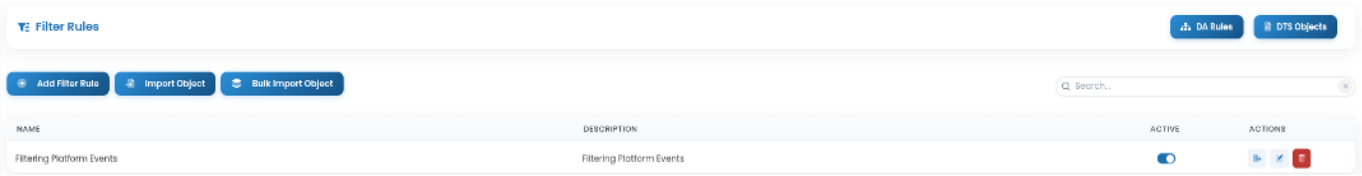
To see how to create a parser, please follow the link: How to create a parser.

Filter rules

CYBERQUEST uses an intelligent event filter mechanism for sending data to JS parsers. You can instruct DTS on how to filter events sent to parsers by creating filter rules.

Filter rules can be managed by navigating to **Settings > Rules > Filter Rules**. **Filter Rules** page opens allowing rules to be defined based on operators like “eq”, “noteq”, “isInList”, “isNotInList”, “startsWith”, “endsWith”, etc. There is practically no limit to adding additional fields.

The **Actions** menu includes options for edit, delete or export a rule, and you can mark rules as active or inactive. **Filter Rules** page opens, listing defined rules and here you have options for importing an object or creating a new filter rule from scratch.



To export a rule, press



button next to it. The export is saved as a proprietary CQO file. Likewise, to import a rule select



in **Filter Rules** page.

To edit details for a specific rule, press



button next to it. **Edit Filter Rule** page opens allowing you to change the **Filter Name** and **Description**, as well as add, correct or delete already defined filters.

To delete a rule from the list, press



button next to it. As a measure of precaution, you will be asked to confirm deletion.

To mark a rule as activate/inactivate, press



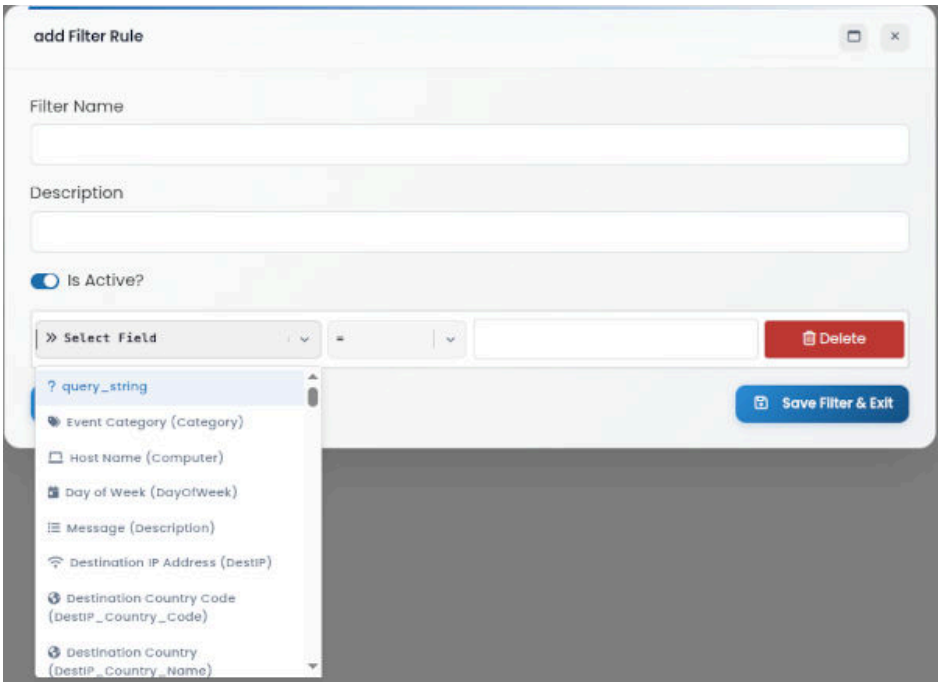
button.

Creating a new filter rule

In **Filter Rules** page, select



button and configuration page opens allowing you to create a new rule:



Complete the following fields:

- In **Filter Name** field, type a name that identifies the newly created filter rule
- In **Description** field, insert a description of the filter rule
- Press **Add field condition** button to define one or more condition to filter data

A filter rule can have one or more condition defined:

- In **Select Field** drop-down list, select the event field you want to filter
- In **Operator** drop-down list select from one of the available operators **eq**, **noteq**, **isInList**, **isNotInList**, **startsWith**, **endsWith**, **etc**.
- Type in the **Value** used for comparison

By default, the new rule will be active. Press on



switch to inactivate the rule.

At any moment you can press



to delete a filter.

When you finished creating the rule, press

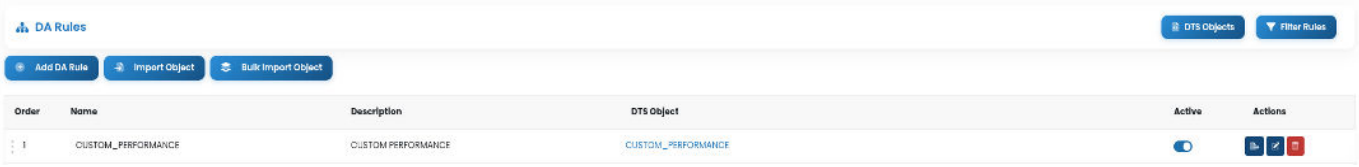


button to save changes and return to rules list.

Data acquisition rules (DA Rules)

CYBERQUEST includes a decisional engine based on rules that allows to combine filter rules with JS parsers for the purpose of establishing a granular data collection flow. As such, for a given flow of events, you will be able to assign one or more parsers to specific filtering rules and this way instruct the platform on what events will be collected.

Data acquisition rules can be accessed from Web Interface by navigating to **Settings > Rules > DA Rules**. **DA Rules** page opens, listing defined rules, and here you have options for importing and object or creating a new DA rule from scratch. The **Actions** menu includes options for edit, delete or export a rule, and you can mark as active or inactive.



- To export a rule, press

  button. The export is saved as a proprietary CQO file. Likewise, to import a rule select

  in **DA Rules** page.

- To edit details for a specific rule, press

  button. **Edit DA Rule** page opens allowing you to change the Name and Description, as well as add, correct or delete already defined filters.

- To delete a rule from the list, press

  button next to it. As a measure of precaution, you will be asked to confirm deletion.

- To mark a rule as activate/inactivate, press

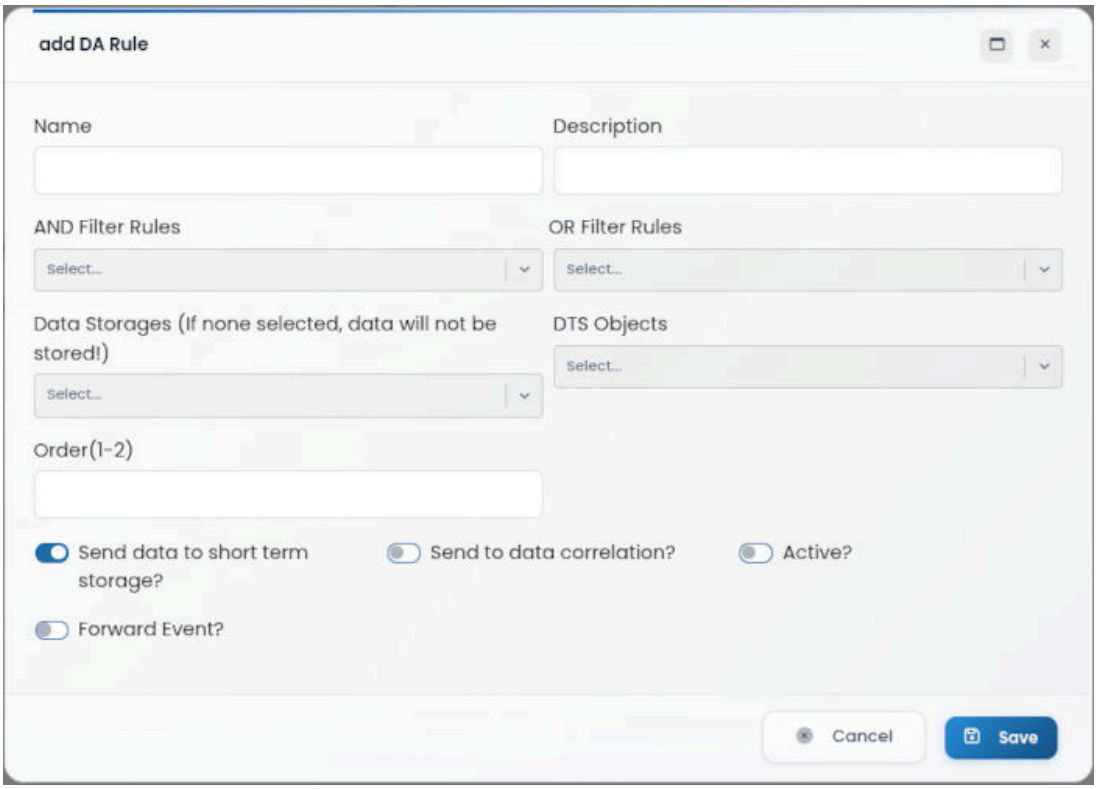
  button.

Creating a new DA rule

In **DA Rules** page, select



button and configuration page opens allowing you to create a new rule:



Complete the following fields:

- In **Name** field, type a name that identifies the newly created data acquisition rule (appears in **DA Rules** list)
- In **Description** field, insert an explanatory rule description
- **AND filter rules** apply logical AND operators to combine multiple filtering conditions
- **OR filter rules** apply logical OR operators to handle alternative filtering conditions
- **Data Storages** lets you select long-term storage destinations
- In **DTS Objects** drop-down list, select the DTS objects this rule applies to
- In **Order** field, set processing priority (lower numbers execute first)
- **Send data to short term storage** routes events to Online DataStorage database
- **Send to data correlation** forwards data to data correlation service
- **Active** toggles rule activation status
- **Forward Event**: enables forwarding of events to a syslog server.

After a DA Rule is created, the “Save” button stores the changes, while the “Cancel” button discards them.

User and Group Management

Role-Based Access Control (RBAC)

CYBERQUEST implements Role-Based Access Control (RBAC) to manage user permissions through predefined roles. This security model allows administrators to:

- Assign granular permissions to user groups
- Control access to web interface components
- Maintain consistent access policies across the organization

Administrators can create new roles or modify existing ones to meet specific security requirements.

Create or Modify User Roles

To create or modify user roles:

1.Log in with administrative privileges

2.Navigate to **Settings > Users and groups > Groups**

3.Create a new group or edit an existing one

4.In the **Assigned Permissions** field, select appropriate access rights

5.In the **Data Permissions** field, define data access filters

Roles are always assigned at the group level, not directly to individual users.

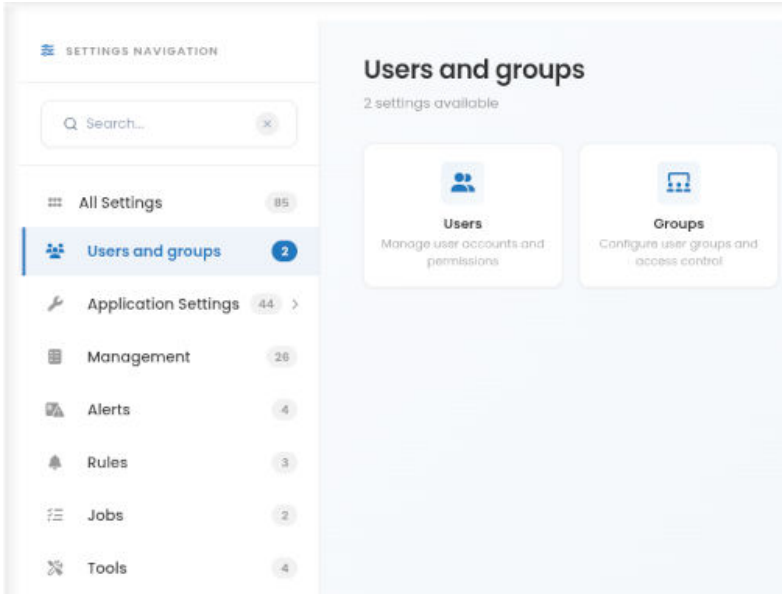
To add or edit user roles:

1.Log in to the application with an administrative account.

2.Navigate to **Settings** by clicking the



button on the left side of the interface, then select **Users and groups > Groups**.



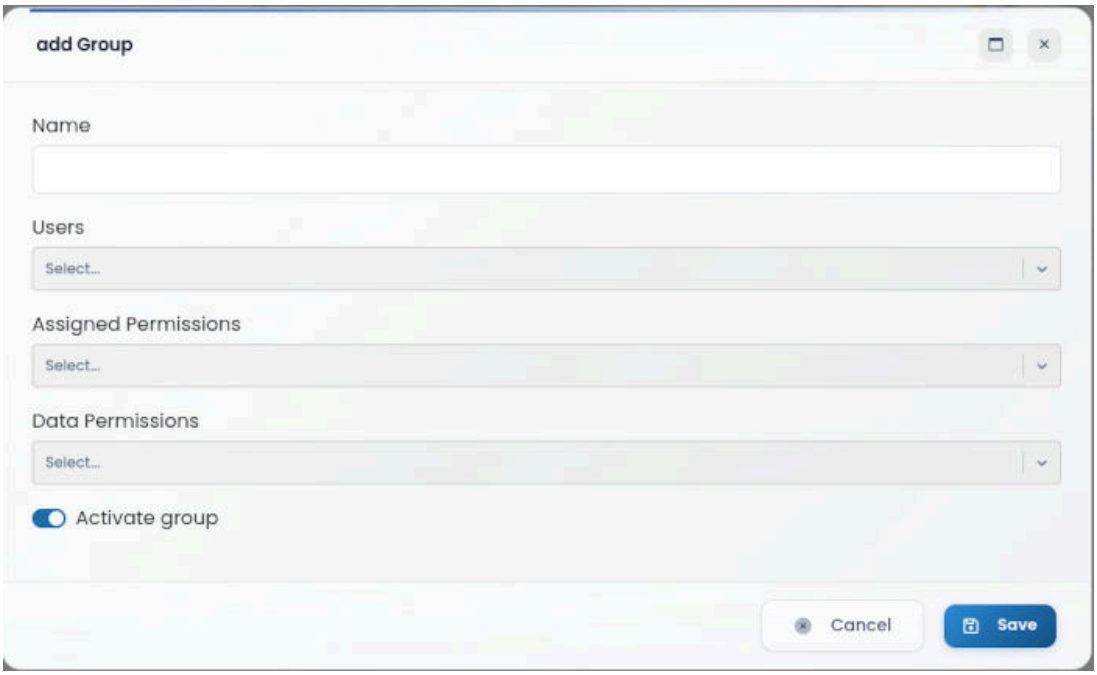
3.The **Groups** configuration page opens:



4.In the **Groups** window, click the



button to open the group creation form:



- In the **Name** field, provide a descriptive name (e.g., “Critical Assets Monitoring”).
- In the **Users** field, select the users affected by the predefined rules.
- In the **Assigned Permissions** field, select appropriate permissions for the selected users.
- In the **Data Permissions** field, select the data accessible to the selected users.
- By default, new groups are enabled. Deactivate a group by selecting the

  Activate group

  option.

Press “Save” to create the new group or “Cancel” to discard changes. Alternatively, close the window without saving by clicking the

×

mark in the top-right corner.

Delete User Groups

To delete a group:

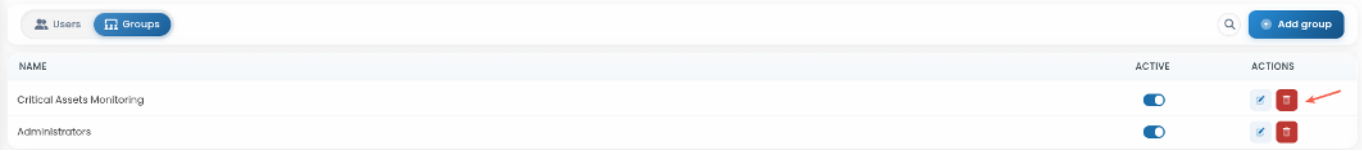
1. Navigate to **Settings** by clicking the

   Settings

   button on the left side of the interface, then select **Users and groups > Groups**.
2. Click the

   button next to the desired group and confirm deletion.

Note: This procedure is irreversible. Built-in groups cannot be deleted.



Edit User Groups

To edit a group:

1. Navigate to **Settings** by clicking the

   Settings

   button on the left side of the interface, then select **Users and groups > Groups**.

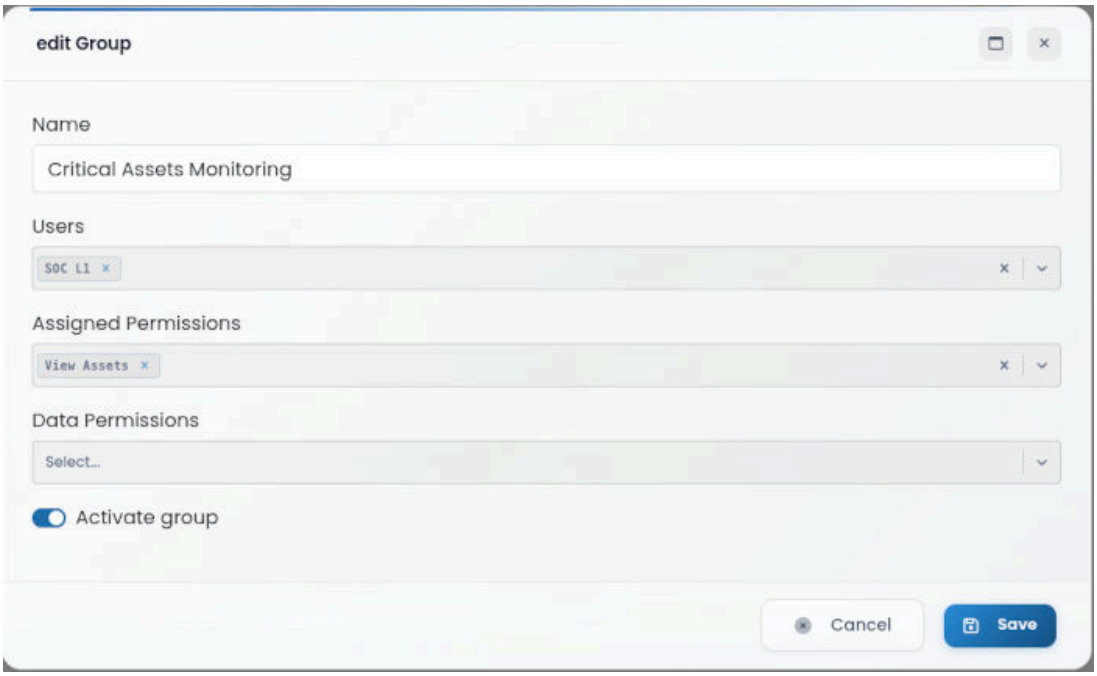
2. Click the

   button next to the desired group.

3. The Edit Group window displays options to modify the group name, users, assigned permissions, and data permissions.



Changing group users, assigned permissions and data permissions is one by selecting or de-selecting objects in each drop-down list.



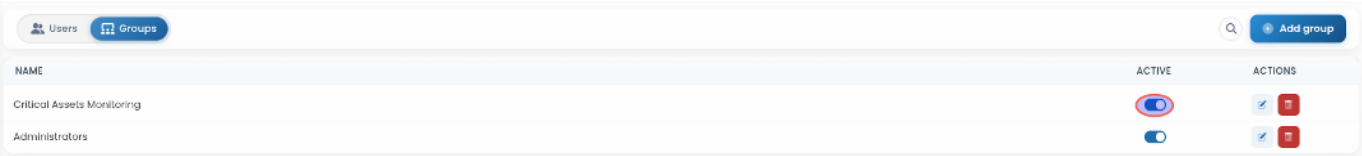
Press the “Save” button to apply changes and close the window, or press “Cancel” to close the window without saving. Alternatively, the window can be closed without saving changes by clicking the

×

icon in the top-right corner.

You can also change group status being **Enabled** or **Disabled**. Group status can be quickly changed from main Groups window by actioning on **Active** option button and selecting **On** or **Off**. In this case, changes are saved automatically.

The group status can be set to either **Enabled** or **Disabled**. Changes are made directly from the main Groups window using the **Active** option button (On/Off) and are saved automatically.



For built-in groups, only adding or removing users is permitted.

Dashboard Migration

Administrators can migrate dashboard configurations between user accounts to:

- Streamline onboarding of new users
- Maintain consistent visualization standards
- Transfer expert configurations to new team members

To migrate dashboards:

1.Log in with administrative credentials

2.Navigate to **Settings > Users and groups > Users**

3.Select the target user account

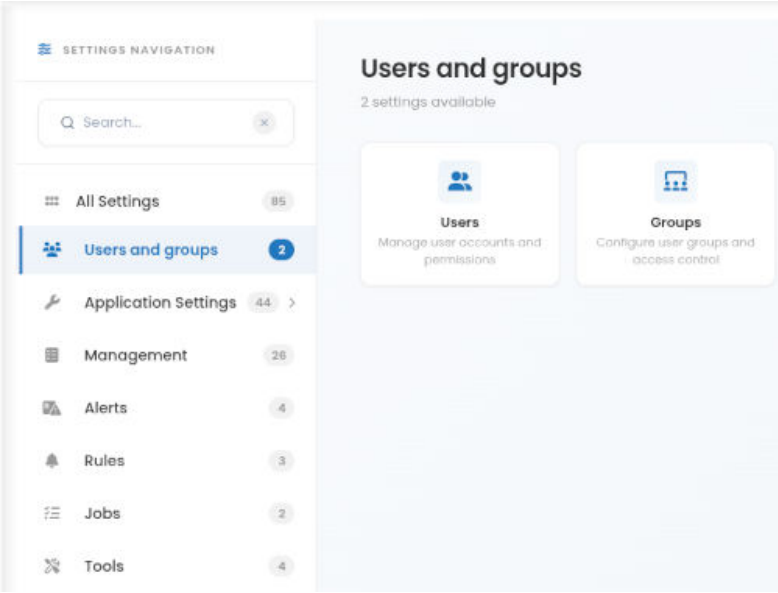
4.Choose **Copy dashgroups to user** from the available actions

1.Log in to the application with an administrative account.

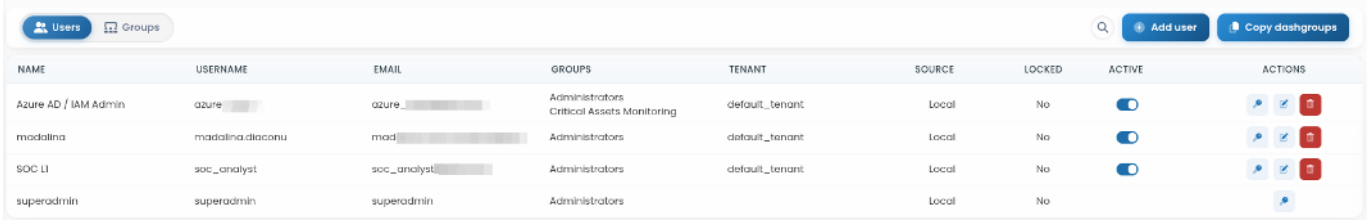
2.Navigate to **Settings** by clicking the



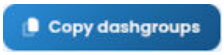
button on the left side of the interface, then select **Users and groups > Users**.



3.On the **Users** configuration page, select **Copy dashgroups to user**:



4.Click the



button to open the copy dialog:



- Select source and destination users from the **User where dashgroups are copied from** and **Users where to copy dashgroups** dropdown lists.
- Choose desired dashgroups from the **Dashgroups that are copied** dropdown list and press “Save” to apply changes.

Log out from the administrative account and log in with the new user account. The Dashboards module will display the copied dashgroups.

Data Permissions

Data permissions work in conjunction with role-based access controls to provide granular data visibility management. These permissions are configured at the group level to:

- Restrict data access by category
- Implement need-to-know basis security
- Enforce data governance policies

To configure data permissions:

1.Log in with administrative privileges

2.Go to **Settings > Users and groups > Groups**

3.Edit the target group

4.In the **Data Permissions** section, select appropriate data filters

5.Save changes to apply new permissions

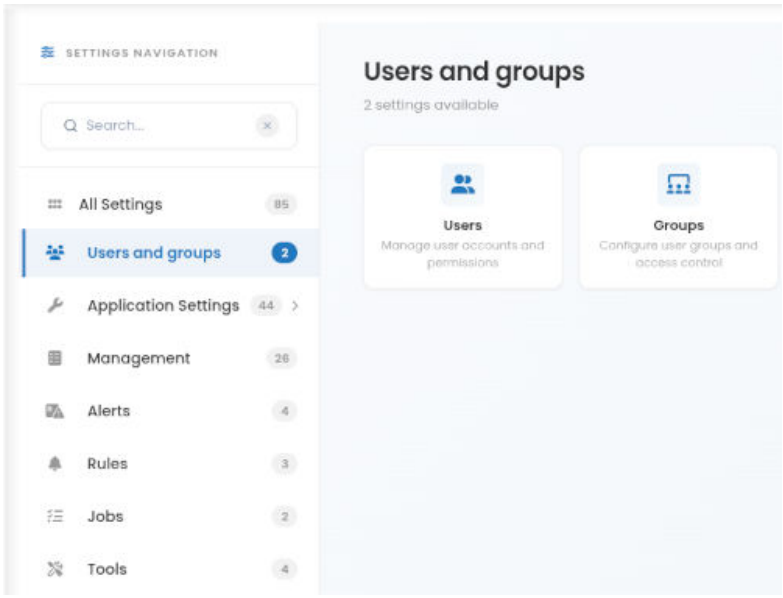
To configure data permissions for an existing group:

1.Log in to the web interface with administrative rights.

2.Navigate to **Settings** by clicking the



button on the left side of the interface, then select **Users and groups > Groups**.



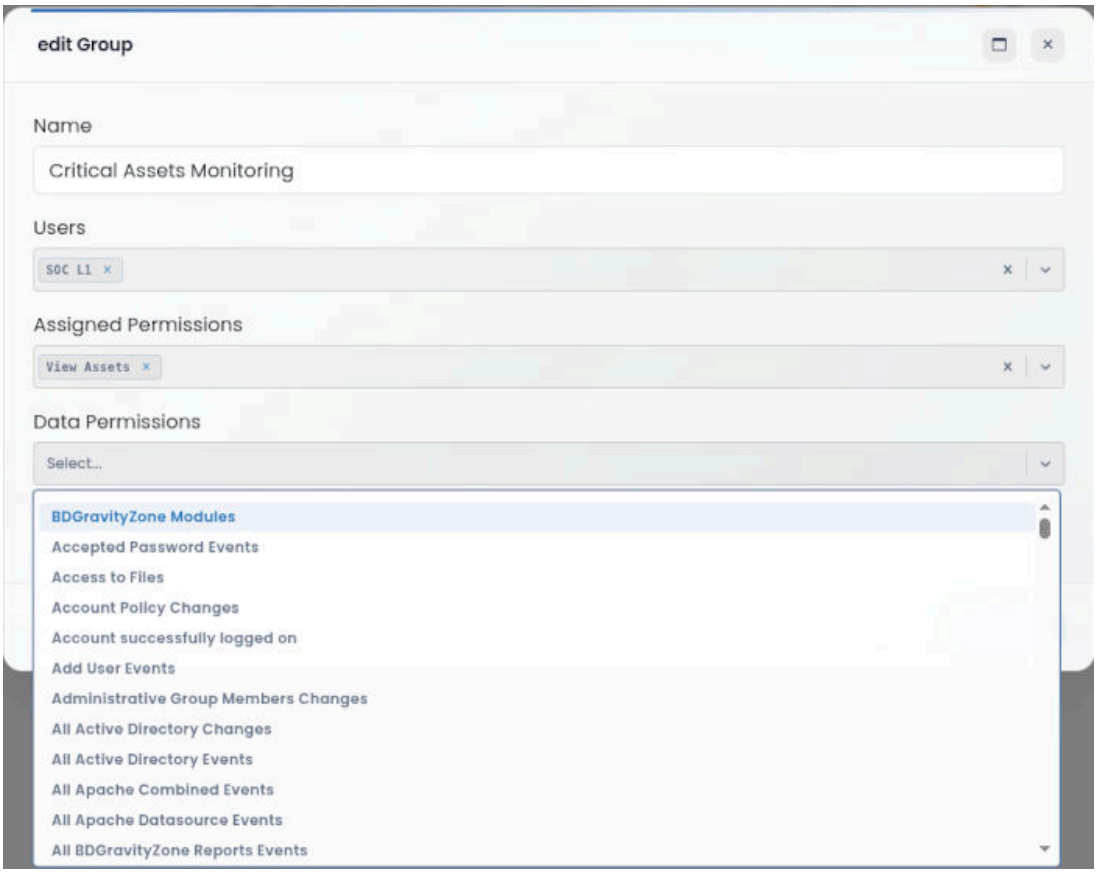
3.In the **Groups** window, click the



button for the target group. The **Edit group** window opens.



4.In the **Data Permissions** field, select or deselect appropriate data filters. Without any filters, users have unrestricted access to all available data.



Press “Save” to apply changes or “Cancel” to discard them. Alternatively, close the window without saving by clicking the



mark in the top-right corner.

Data Scanner

Data Scanner

The **Data Scanner** module performs agentless active collection. It queries network devices and applications directly, using standard protocols, and stores the results in the CYBERQUEST platform. No software component has to be installed on the monitored device.

To access this section, open **Settings** from the left-side navigation menu, then select **Application Settings > Data Scanner**.

The module is organized into six tabs:

- **Targets** - Defines what is queried, how often, and with which credentials.
- **Devices** - Lists the devices discovered by the scans and their configuration inventory (CMDB).
- **Availability** - Shows the reachability state of the monitored services.
- **Routing** - Shows the state of the BGP sessions and OSPF adjacencies of the monitored devices.
- **Config** - Stores network device configurations and the differences between versions.
- **Alerts** - Defines alerting rules on the collected values.

The header of the page shows the total number of targets, how many are active, how many are healthy, and how many report issues.

Targets

A **target** is one collection job: a host, the protocol used to query it, the schedule, and the credential. To add one, go to **Settings > Application Settings > Data Scanner > Targets** and click **Add target**.

The following fields are available:

- **Name** - A label used to identify the target in the interface.
- **Kind** - The collection type. Determines which protocol is used and what is collected.
- **Host** - The IP address or hostname of the device or application to query.
- **Port** - The port on which the service listens. When left empty, the default port of the selected protocol is used.
- **Credential** - The credential used for authentication, selected from the platform credential store. Credentials are stored encrypted and are never displayed in clear text.
- **Schedule** - The collection frequency, expressed in cron format.
- **Parameters** - Additional options specific to the selected collection type.

The available collection types are:

- **snmp** - Device classification and performance metrics over SNMP v2c or v3.
- **availability** - Service reachability checks (ICMP, TCP, Telnet and other services).
- **route** - BGP and OSPF neighbor state.
- **config** - Retrieval of the running configuration of a network device.
- **ssh** - Host metrics and running processes on Unix and Linux systems.
- **wmi** - Host metrics and running processes on Windows systems.
- **jdbc** - Availability and metrics of a database instance.
- **jmx** - Java application metrics, collected over Jolokia.
- **vmware** - Host and virtual machine inventory, collected through the VMware SDK.

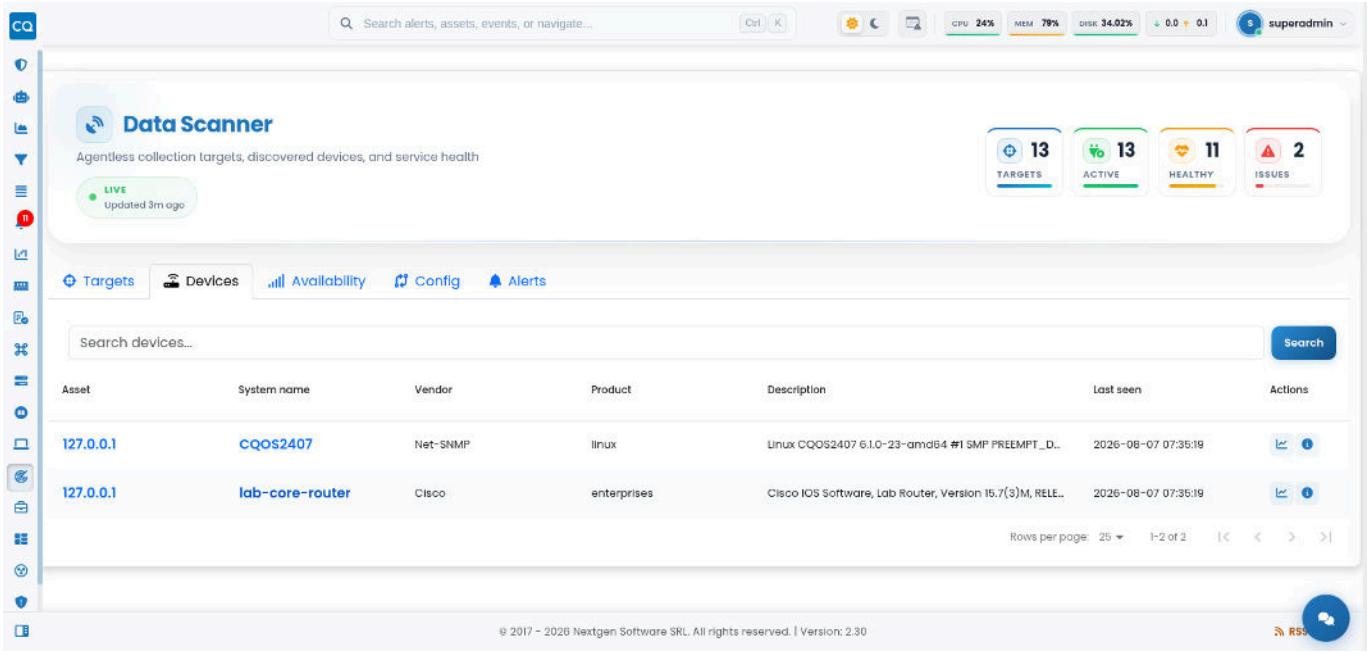
Each target can be activated or deactivated from the **Actions** column. The **Run now** action starts a collection immediately, without waiting for the next scheduled run, and is useful for validating a newly added target. The **Test connection** action verifies that the host is reachable and that the credential is accepted, without storing any data.

Devices

The **Devices** tab lists the devices discovered during the scans. Discovery is automatic: a device appears here after the first successful collection, without operator intervention.

The table displays the following columns:

- **Asset** - The address at which the device was reached.
- **System name** - The name reported by the device.
- **Vendor** - The manufacturer, resolved from the device identifier.
- **Product** - The product family reported by the device.
- **Description** - The system description reported by the device.
- **Last seen** - The moment of the last successful collection.



The **Actions** column provides access to the performance metrics of the device and to the device details page.

Device details (CMDB)

Clicking a device opens its detail page, which lists the configuration inventory maintained locally by the platform for that device. The information is obtained exclusively from the device itself, through standard protocol queries, and is refreshed at every collection cycle.

The page is organized into three sections.

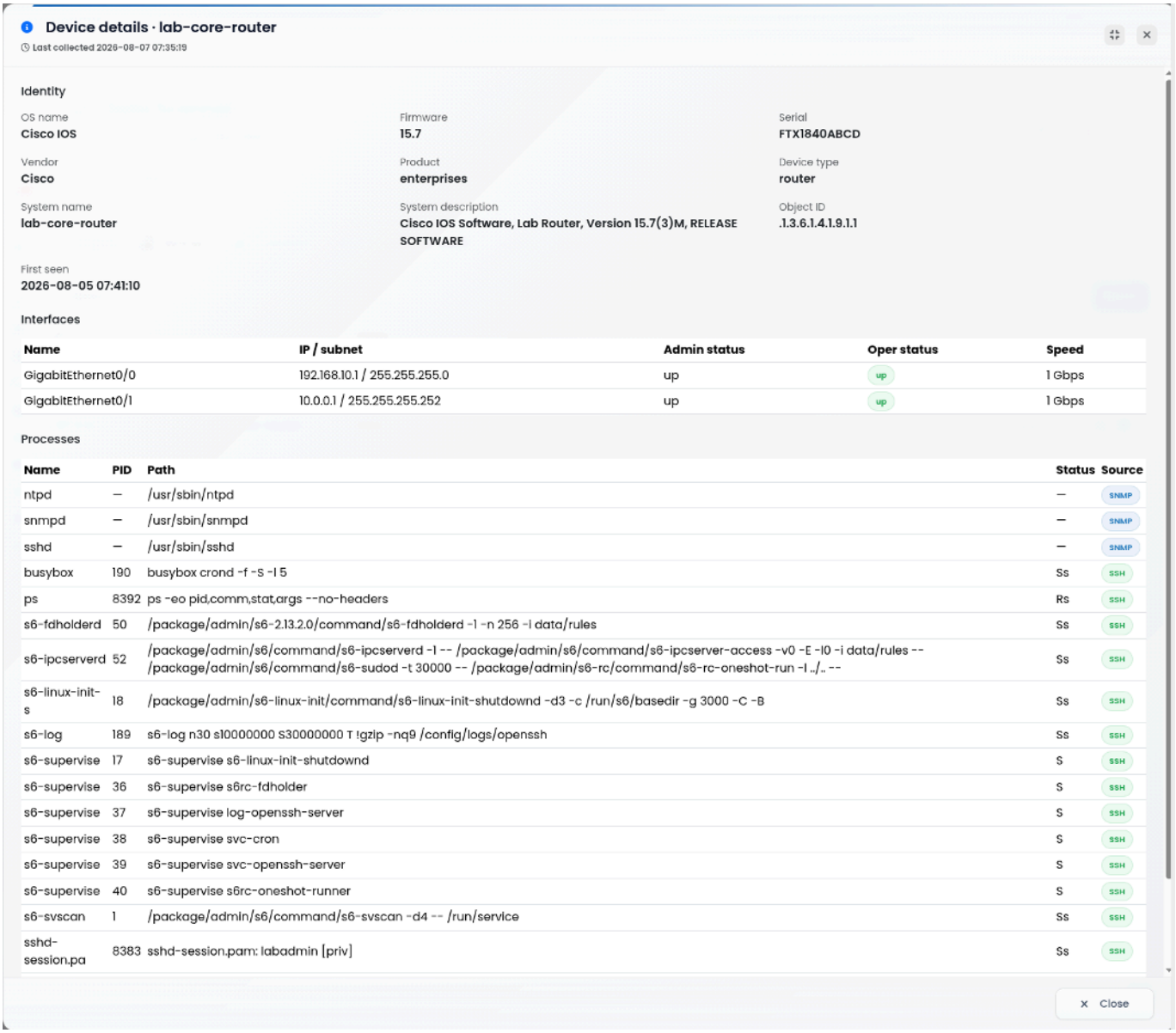
Identity - Contains the identification data of the device:

- **OS name** - The installed operating system.
- **Firmware** - The firmware or software version.
- **Serial** - The serial number of the device.
- **Vendor**, **Product**, **Device type** - The manufacturer, product family, and device category.
- **System name**, **System description**, **Object ID** - The values reported by the device.
- **First seen**, **Last collected** - The moment of the first discovery and of the last successful collection.

Interfaces - Lists the configured interfaces of the device:

- **Name** - The interface name.
- **IP / subnet** - The IP address and the allocated subnet mask.
- **Admin status** - The administrative status of the interface (enabled or disabled).
- **Oper status** - The operational status of the interface.
- **Speed** - The transmission speed of the link.

Processes - Lists the processes running on the device or operating system, with the process name, PID, executable path, status, and the **Source** column, which indicates the protocol through which the process was discovered. A device queried through several protocols has its process list consolidated per asset, and each entry remains traceable to the collection method.



Values that the queried device does not expose are left empty. The platform does not infer or complete missing values, so the inventory reflects only information reported by the device.

Performance metrics

Devices that report numeric values expose them as metrics. To view them, open the **Devices** tab and use the metrics action on the device row. The **Device metrics** panel opens, showing one chart per metric.

The panel provides:

- **Time window** - The period covered by the charts: **6h**, **24h**, or **7d**.
- **Pin metric** / **Unpin metric** - Selects which metrics stay on screen. Pinned metrics are remembered for the next visit, per user and per device, so each operator keeps their own working set.
- **Maximize** / **Restore** - Enlarges the panel for detailed reading.

Each chart shows the number of samples it contains. When a device has not reported numeric values in the selected period, the panel states this and suggests widening the window or running a scan.

The metrics available depend on the collection type of the target:

Collection type	Metrics collected
snmp	Processor load, memory used, uptime, number of interfaces, number of interfaces in the up state
wmi	Processor load, number of logical processors, total and free memory, total and free disk space, total and running services
jdbc	Number of rows returned, plus every numeric column of the configured query

Metric collection is best-effort: a value the device does not expose is simply omitted from that collection cycle. A missing value never causes the scan to fail, and the device continues to report the metrics it does support.

Categories

Every device the platform reaches is classified automatically at each collection cycle, without operator intervention. Two independent values are recorded.

The **device type** is a best-effort value derived from what the device itself reports — its system description and, over SNMP, its object identifier resolved through the platform's MIB database. It carries a confidence score and is left empty when the device exposes nothing to derive it from.

The **category** groups devices for listing and is always determined, because it follows from the protocol used to reach the device. Four categories exist:

- **Network equipment** - routers, switches, firewalls and access points.
- **Servers and workstations** - hosts reached over WMI or SSH, ESXi hosts and virtual machines retrieved through the VMware SDK, and servers identified over SNMP.
- **Applications** - database instances reached over JDBC, Java applications reached over JMX, and the vCenter endpoint. This category also lists the software discovered in the processes collected from monitored hosts; because that software was not queried directly, no version is reported and operating-system processes appear alongside applications.
- **Other equipment** - printers, UPS units, cameras, and devices that could not be identified.

In the **Devices** tab, the category filter above the table lists the number of devices in each category and restricts the table to the selected one. Both the device type and the category are also available as sortable columns.

Availability

The **Availability** tab shows the reachability state of the monitored services. It contains two tables.

Availability levels summarizes uptime over a selected period. Use the **Availability period** control to switch between **24h**, **7d**, and **30d**. The table lists:

- **Asset** - The address of the monitored device.
- **Service** - The checked service.
- **Availability** - The percentage of successful checks in the period. The value is shown in green at or above 99.9%, in amber at or above 99%, and in red below that.
- **Last outage** - The moment the most recent interruption started.
- **Longest outage** - The duration of the longest interruption in the period, shown in a readable form such as `2h 3m`.

The second table shows the current state, with one row per monitored service:

- **Asset**, **Service** - The device and the checked service.
- **Status** - **up**, **down**, or **degraded**.
- **RTT** - The response time in milliseconds, shown only for services in the up state.
- **Last change** - The moment of the last state change.
- **Last checked** - The moment of the last verification.

The table can be searched and sorted, and the **Refresh** button reloads the latest results.

Each check is performed with the protocol of the service, not only with a generic connection attempt. The services that can be verified are **icmp**, **dns**, **tcp**, **udp**, **telnet**, **ssh**, **scp**, **ldap**, **http**, **https**, **ftp**, **smtp**, **imap**, **pop3**, **pop3s**, and **jdbc**. **tcp**, **udp**, and **jdbc** are generic probes and require an explicit port; every other service uses its standard port unless one is configured. **scp** has no listener of its own — it runs over the SSH transport, so it is verified on port 22 in the same way as **ssh**. A single availability target can verify several services, and each of them can use its own port, so the same device can be checked on several services in one collection cycle.

Routing

The **Routing** tab shows the current state of the dynamic routing protocols on the monitored network devices. It lists one row per routing neighbour, so the state is reported per session rather than as a single verdict for the whole device:

- **Asset** - The address of the monitored device.
- **Protocol** - **BGP** or **OSPF**.
- **Peer** - The address of the neighbour.
- **State** - The state of the BGP session or of the OSPF adjacency, shown under its standard name. A session in **established** and an adjacency in **full** are shown in green; a session in **idle** and a neighbour in **down** are shown in red; the transitional states through which a session passes while it is being set up are shown in amber.
- **Last change** - The moment the neighbour last changed state.
- **Last checked** - The moment of the last verification.

The table can be searched and sorted, and the **Refresh** button reloads the latest results.

The state is read from the standard objects through which the two protocols expose it - `bgpPeerState` for BGP sessions and `ospfNbrState` for OSPF adjacencies - so it is obtained in the same way from any device that implements these MIBs, whichever the manufacturer. The numeric values reported by the device are converted to the standard state names, and the whole BGP state machine and OSPF adjacency state machine are covered.

Last change is only moved forward when the state actually changes. A neighbour that keeps the same state from one cycle to the next has only its **Last checked** updated, which makes it possible to tell not just what the state is, but how long the neighbour has been in it.

A neighbour that the device stops reporting is removed from the list at the next successful collection, rather than being left frozen in its last known state. If instead the device cannot be reached or the collection fails, the list is not emptied: the last known state is kept, and **Last checked** stops advancing, which shows that the information has not been refreshed.

Which protocols are polled is chosen per target, from the **Routing protocols** checkboxes of a target of kind **route**. A neighbour of a protocol that is no longer selected disappears from the list at the next collection, so the tab never shows state that is no longer being monitored.

Config

The **Config** tab stores the configurations retrieved from network devices and shows the differences between versions.

At every collection, the platform retrieves the running configuration of the device and compares its fingerprint with the previously stored version. **A new version is stored only when the configuration has actually changed.** A device that stays unmodified therefore produces no new entries, no matter how often it is scanned, and the history contains only genuinely distinct versions.

The command used to retrieve the configuration is selected automatically according to the device manufacturer, as identified by the SNMP scan. It can also be set explicitly from the target parameters, for devices that require a specific command.

Host-key verification

Configuration retrieval over SSH verifies the identity of the device before the credential is sent. Two target fields control this:

- **SSH host-key policy** - **Strict verification**, the default, accepts the connection only when the device's host key is already known. **Insecure (skip host-key check)** disables the verification and is intended for testing only.

- **Known-hosts file** - The path, inside the platform, of the file holding the accepted host keys. The default is `/etc/data-scanner/known_hosts`.

Until the device's key is present in that file, a target on strict verification fails with `key is unknown`. Entries are produced with the standard `ssh-keyscan` utility, one line per device:

```
ssh-keyscan 192.0.2.10 >> /etc/data-scanner/known_hosts
```

The known-hosts file has to exist before the service is started for the first time. In a container deployment the file is supplied from the host; if the host path does not exist, the container runtime creates a *directory* in its place and every target on strict verification then fails with `known-hosts: ... is a directory`. Creating an empty file before the first start avoids this.

Comparing configurations

The **Compare configurations** panel takes:

- **Config target** - The device whose history is examined.
- **Older version** and **Newer version** - The two versions to compare, identified by their collection moment and the beginning of their fingerprint.

Click **Compare** to display the differences. Added lines are marked with `+` on a green background, removed lines with `-` on a red background, and the header of the result shows the number of added and removed lines. When the two selected versions have identical content, the interface states this explicitly instead of showing an empty result.

Very large differences are truncated for display, and a notice indicates that only the first part of the difference is shown.

Version history

The lower table lists the stored versions:

- **Collected** - The moment the version was retrieved.
- **Method** - The protocol used, **SSH** or **TELNET**.
- **Size** - The size of the stored configuration.
- **SHA-256** - The fingerprint of the version, used to distinguish it from the others.

The two versions currently selected for comparison are highlighted. Older versions are loaded on demand with the **Load older versions** button.

If no target of type **config** exists yet, the tab explains what has to be configured before configuration history becomes available.

Alerts

The **Alerts** tab defines alerting rules on the values collected by the module. Rules are evaluated at every collection cycle and raise an alert in the platform when the configured condition is met.

To add a rule, click **Add alert rule**. The following fields are available:

- **Name** - The label of the rule. It becomes the name of the generated alert.
- **Tenant** - The tenant the rule belongs to. The rule applies only to targets of that tenant, so the targets it is meant to watch have to be assigned to a tenant as well — a target left without one never raises alerts.
- **Condition** - What the rule watches. See the table below.
- **Scope** - The targets the rule applies to. Leave it empty to apply the rule to every target in the tenant; use Ctrl/Cmd-click to select several targets.
- **Consecutive breaches** - How many successive collection cycles have to breach the condition before the alert fires. This suppresses alerts caused by a single transient sample.
- **Severity score** and **Severity level** - The values carried by the generated alert.
- **Notification emails** - A comma-separated list of recipients. Leave it blank to raise the alert without sending email.

- **Notify on recovery** - Sends a second notification when the condition returns to normal. The recovery alert carries the same name, prefixed to mark it as a recovery.
- **Enabled** - Activates or deactivates the rule without deleting it.

The available conditions are:

Condition	Fires when
Metric threshold	A collected numeric metric crosses a configured value.
Availability	A monitored service is reported as down.
Routing	A BGP or OSPF neighbor leaves its established state.
Config drift	The configuration of a device differs from the previously stored version.
Scan health	The collection itself fails for the target.

For a **Metric threshold** rule, three additional fields appear:

- **Metric key** - The metric to watch. The list offers the metrics reported recently by the monitored equipment; if the metric has not been reported yet, choose **Custom…** and type its name.
- **Operator** - The comparison to apply: `>`, `>=`, `<`, `<=`, or `==`.
- **Threshold** - The value to compare against.

A rule fires once, when the condition has been breached for the configured number of consecutive cycles, and does not fire again while it stays breached. It returns to the normal state as soon as one collection no longer breaches the condition. **Config drift** is an exception: a configuration change is a one-off event, so the rule fires at the first detected change regardless of the configured number of consecutive breaches.

A metric that is not reported in a given cycle does not breach the rule — it is simply skipped, so a device that stops exposing a value does not generate a false alert. To be notified about such a case, use a **Scan health** rule.

Permissions

Access to the module is controlled through two permissions, assigned from the user group configuration:

- **view_data_scanner** - Allows viewing the targets, the discovered devices, the availability state, and the stored configurations.
- **manage_data_scanner** - Allows creating, modifying, and deleting targets and alerting rules.

Management

Management Module

The Management module in CYBERQUEST provides centralized control over all system components, allowing administrators to configure, monitor, and maintain various aspects of the security information and event management platform. This comprehensive guide covers all management functionalities available through the Web Interface.

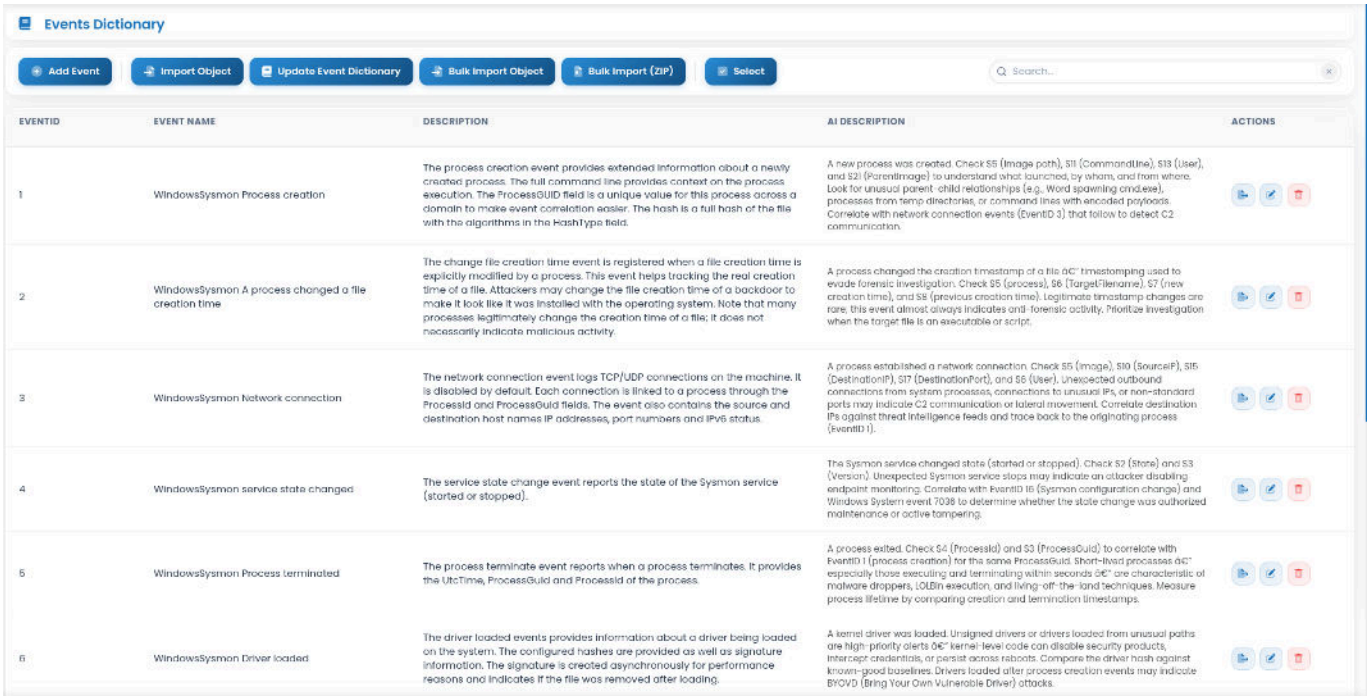
Event Dictionary

The Event Dictionary is a fundamental component of CYBERQUEST that defines how different types of security events are parsed, normalized, and interpreted by the system.

CYBERQUEST includes a comprehensive event dictionary focused on Windows operating systems, with ongoing expansion to cover all major supported technologies. The dictionary is continuously updated to include new event types and security threats.

Accessing the Event Dictionary

Navigate to **Settings > Management > Event Dictionary** in the Web Interface to access the event management page. This interface displays all defined event objects and provides tools for managing them.



- Click the export button

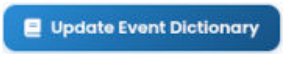
  next to any event definition. Events are exported as proprietary CQO files for backup or sharing.

- To import events, use the import option, by pressing

  button.

- Use the update button

  to refresh the event dictionary with latest definitions.

- Click the edit button

  to modify event properties

- Use the delete button

  to remove event definitions. Confirmation is required before deletion to prevent accidental removal

- Use the Bulk Import button

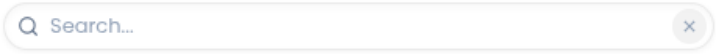
  to select a file and import multiple event definitions. Only files in .cqo format are supported

- Use the Select button



to choose multiple events. The Export option becomes available to export the selected event definitions.

- Use the Quick Filter bar to search by:
  - Event ID
  - Event name
  - Event description



Creating a New Event Definition

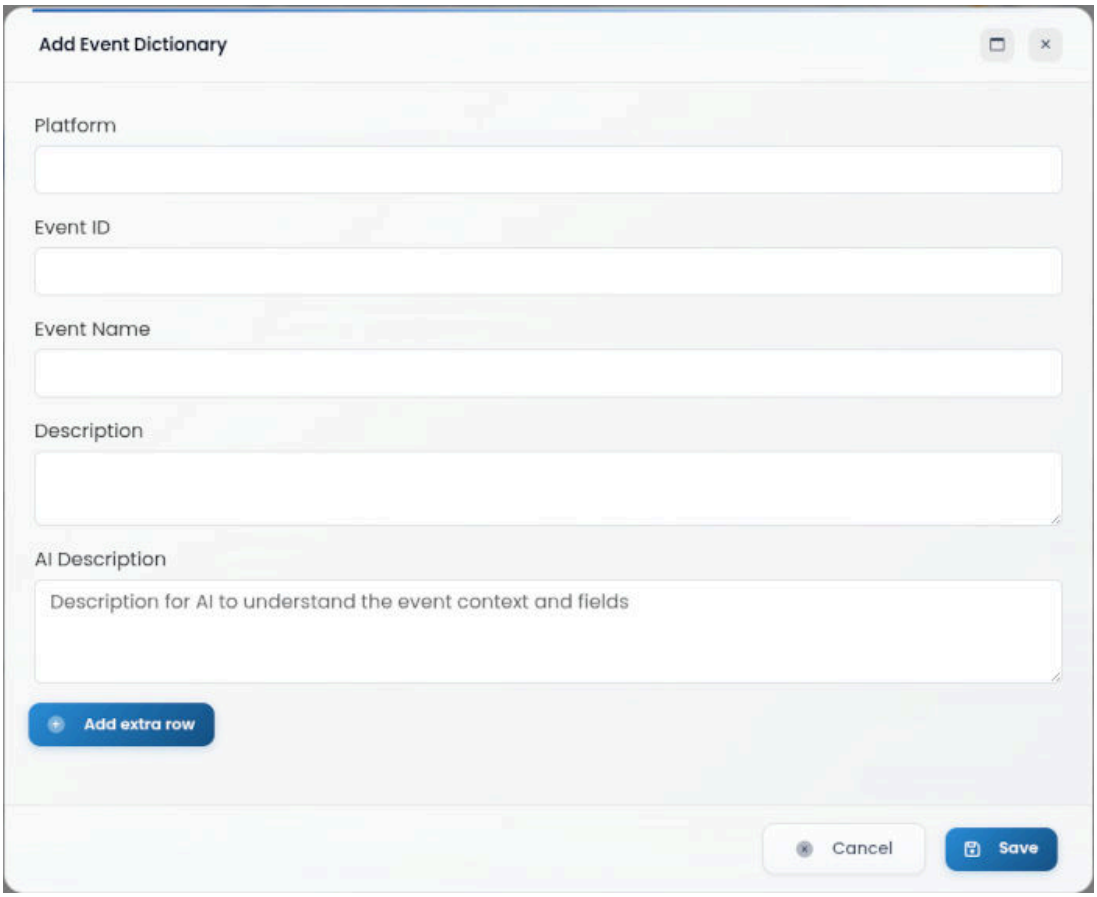
Creating custom event definitions extends CYBERQUEST's capabilities to parse and analyze events from proprietary applications, custom systems, or technologies not covered by the default dictionary.

Access the Creation Interface

- Navigate to **Settings > Management > Event Dictionary**
- From the **Event Dictionary** web interface, select the "ADD EVENT" option



- The **Add Event Dictionary** configuration page will open



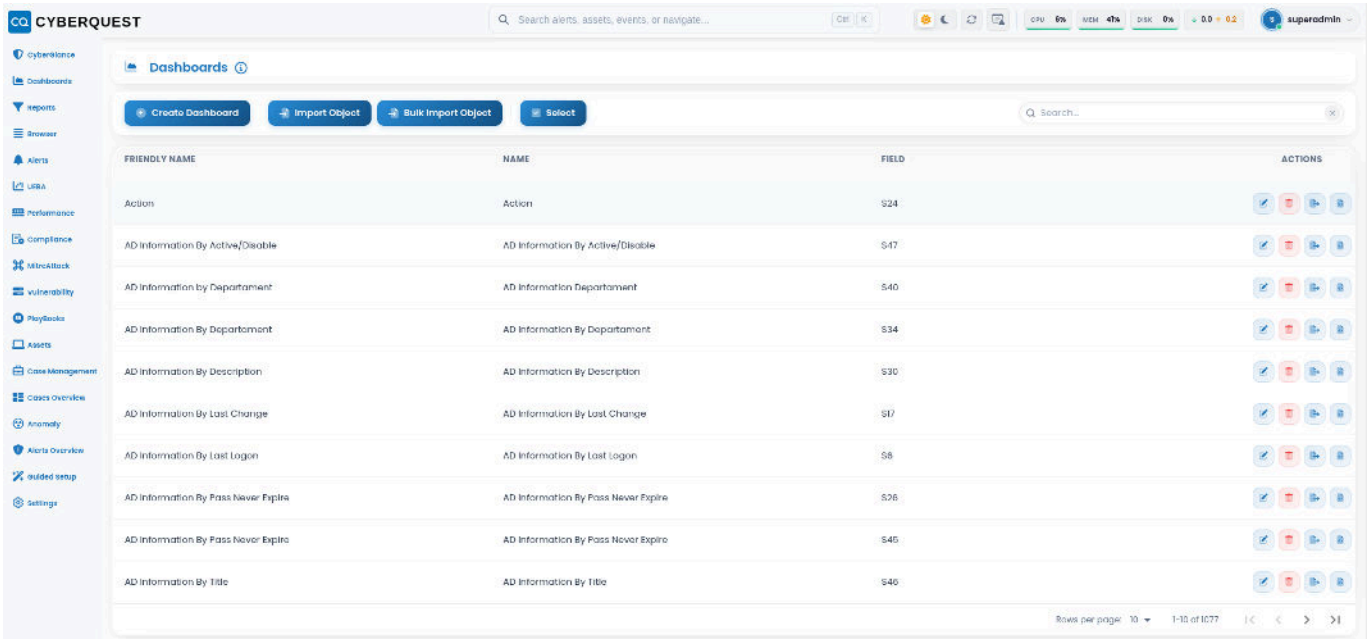
- **Platform**: Technology or system generating the event
- **Event ID**: Unique identifier for the event type (recommend using a standardized numbering scheme)
- **Event Name**: Descriptive name for the event
- **Description**: Detailed explanation of what the event represents
- **ADD EXTRA ROW**: Up to 150 additional fields for event-specific details

After reviewing all configured settings, use the “Save” button to store the new event definition. Once saved, the event becomes immediately available for parsing and analysis.

Managing Dashboards

Dashboards in CYBERQUEST provide visual representations of security data, allowing security teams to monitor key metrics, track incidents, and gain insights into security posture. The Dashboards management interface enables administrators to create, configure, and maintain dashboard configurations for various use cases.

Navigate to **Settings > Management > Dashboards** in the Web Interface. This page displays all dashboard objects configured in your CYBERQUEST instance.



- Click the edit button

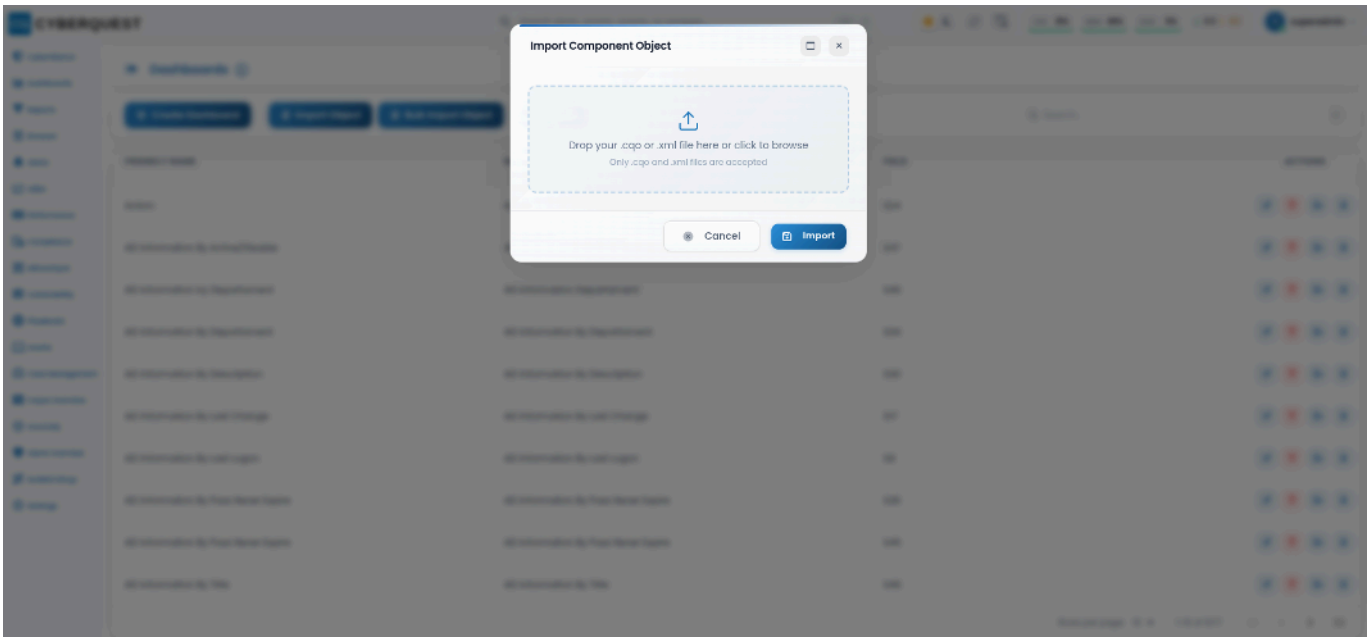
  to modify dashboard properties
- Use the delete button

  to remove dashboards. Confirmation is required to prevent accidental deletion

Import and export dashboards

Dashboard definitions can be imported and exported directly from the Dashboards management interface. To import a dashboard, click **Import Object** and select an `.xml` or `.cqo` file.



To export a dashboard, use the corresponding action available next to the dashboard. Dashboard definitions can be exported either in the CYBERQUEST `.cqo` format using **Export Object**



button, or in XML format using **Export XML**



button.

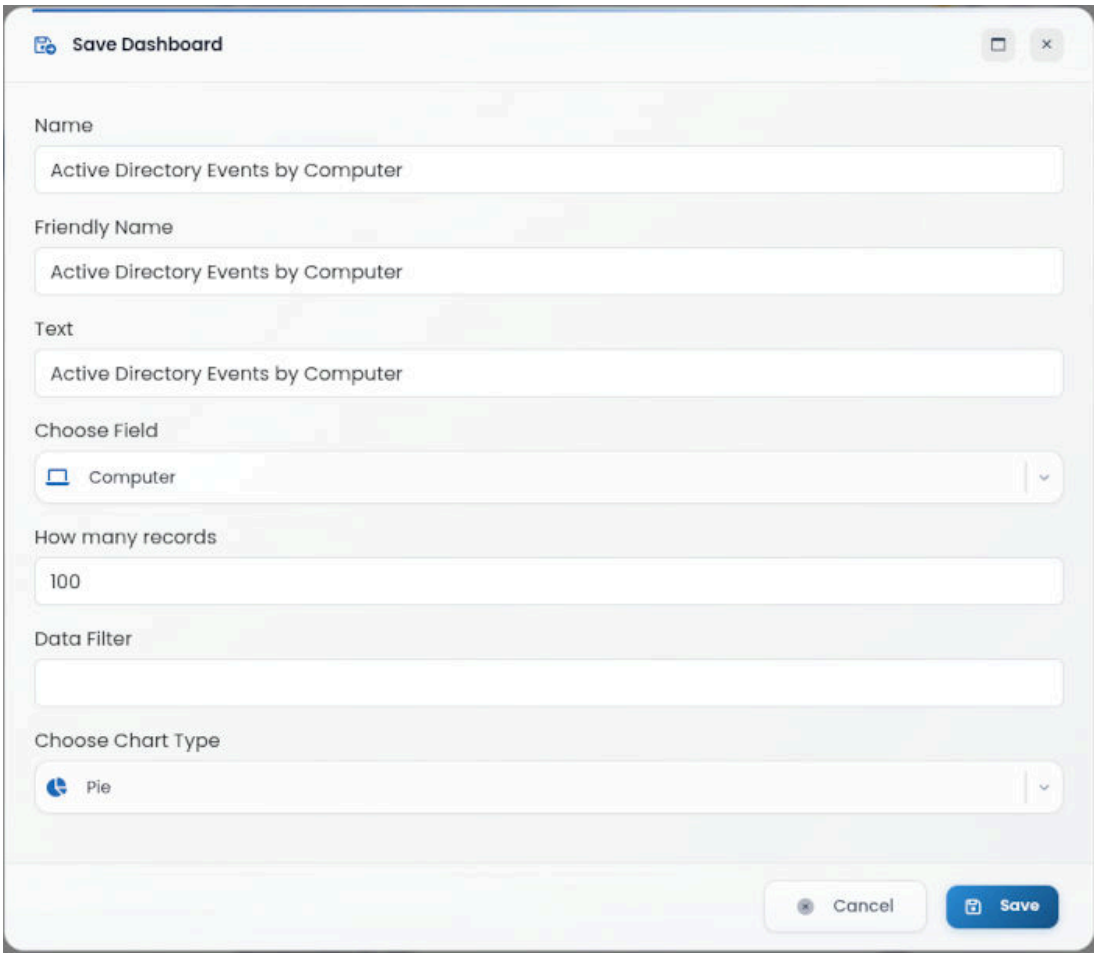
Creating New Dashboards

Click the create button



from the Dashboards management page.

The **Save Dashboard** configuration window will open:



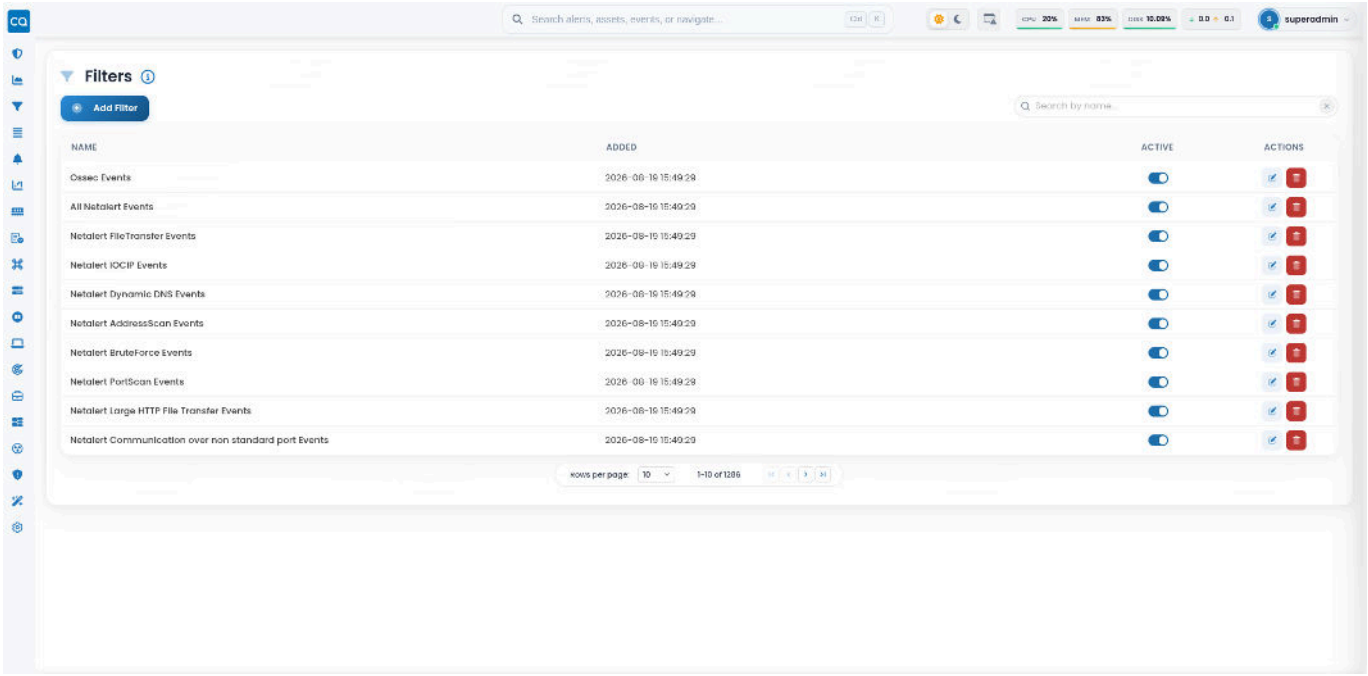
- **Name**: A unique identifier for the dashboard.
- **Friendly Name**: A user-friendly or readable name
- **Text**: Optional descriptive text or notes about the dashboard
- **Choose Field**: Select the specific data field
- **How Many Records**: Specify the maximum number of data entries to display
- **Data Filter**: Apply conditions or criteria to limit which records appear
- **Choose Chart Type**: Select the visualization style

Click “Save” to persist your configuration or “Cancel” to discard changes

Managing Filters

Filters in CYBERQUEST are query-based tools that allow security teams to focus on specific subsets of security data based on defined criteria. They enable precise data filtering for investigations, reporting, compliance monitoring, and threat hunting by applying conditional logic to event streams.

Navigate to **Settings > Management > Filters** in the Web Interface to access the filters management page. This interface displays all configured filter objects.



- Click the edit button



to update an existing filter. Predefined filters follow compliance standards and may require advanced query knowledge.

- Click the delete button



to remove a filter. A confirmation prompt ensures filters aren't deleted accidentally.

- Use the button



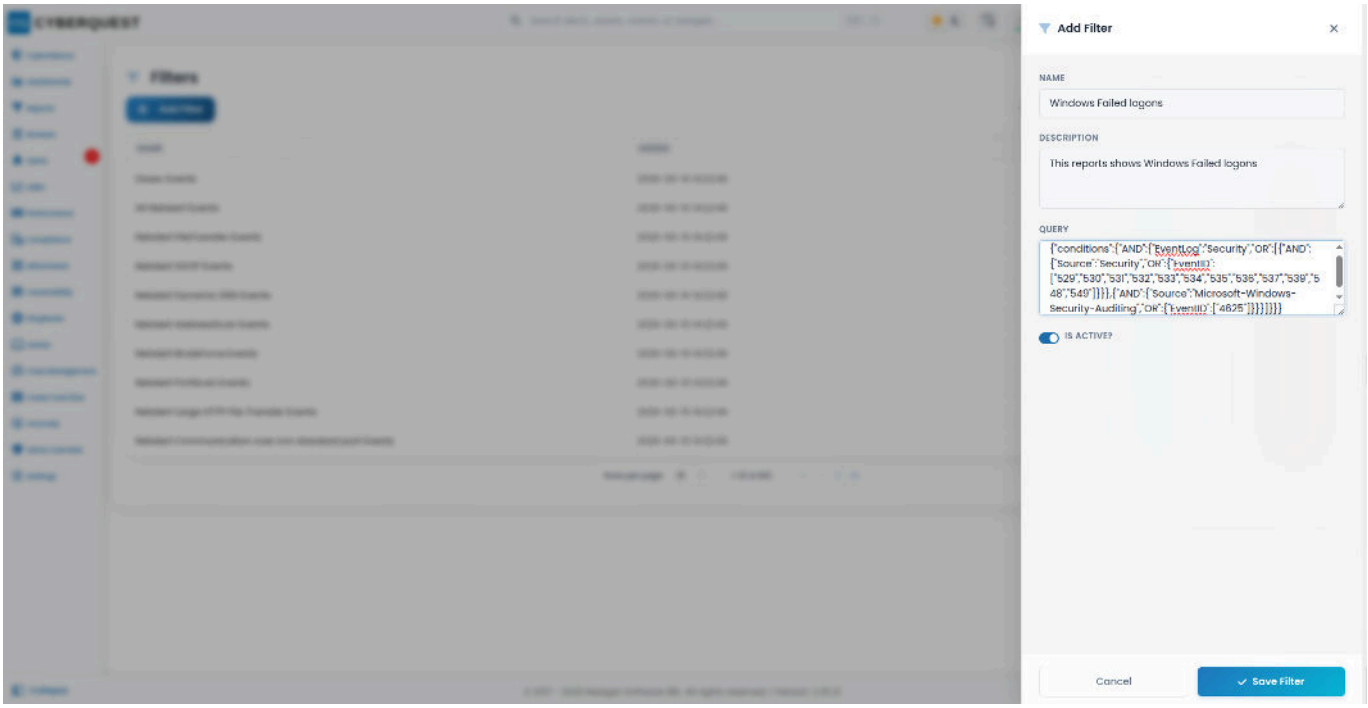
to make a filter active or inactive. Active filters are applied automatically, while inactive filters are saved but not executed.

Creating New Filters

Click the create button



from the Filters management page:



- **Name**: A clear, descriptive title that makes the filter easy to identify.
- **Description**: Details about the filter's purpose.
- **Query**: A CYBERQUEST query language expression that defines the exact criteria for selecting or excluding data.
- **Active/Inactive**: Enables or disables the filter. When active, the filter is applied automatically, when inactive, it is saved but not executed.

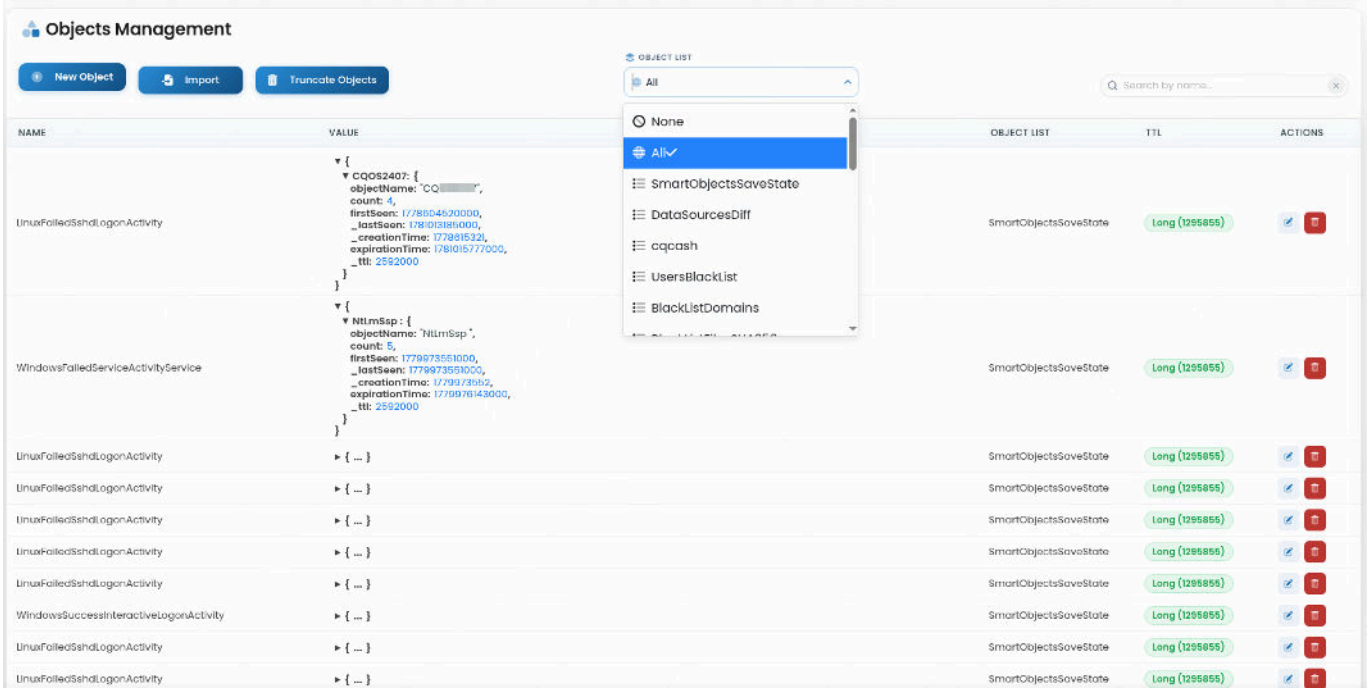
  For detailed instructions on **saving a new filter** from Browser Module, refer to the following link: Save as New Filter.

Managing Objects

Objects in CYBERQUEST represent entities within your IT environment that can be monitored, analyzed, and managed. The Objects Management interface provides centralized control over all object definitions, allowing administrators to create, modify, and maintain object configurations for consistent entity resolution and contextual enrichment across the platform.

- Objects enable consistent identification of entities (users, systems, applications) across different data sources and event types, resolving various identifiers (IP addresses, hostnames, user IDs) to the same logical entity for accurate tracking and analysis
- Objects provide additional context to security events by linking them to known entities, adding information like department affiliation, system criticality, or geographic location to enhance threat assessment and investigation efficiency
- Objects ensure uniform representation of entities in lists, reports, and investigations
- Most objects are created automatically when new entities are detected in the environment
- Administrators can create and modify objects manually for custom or specialized entities

Navigate to **Settings > Management > Objects** in the Web Interface to access the objects management page. This interface displays all object definitions configured in the CYBERQUEST instance. A drop-down list allows viewing all objects or selecting a specific object to display.



- Click the edit button



to modify the details of an existing object in the selected list.

- Click the delete button



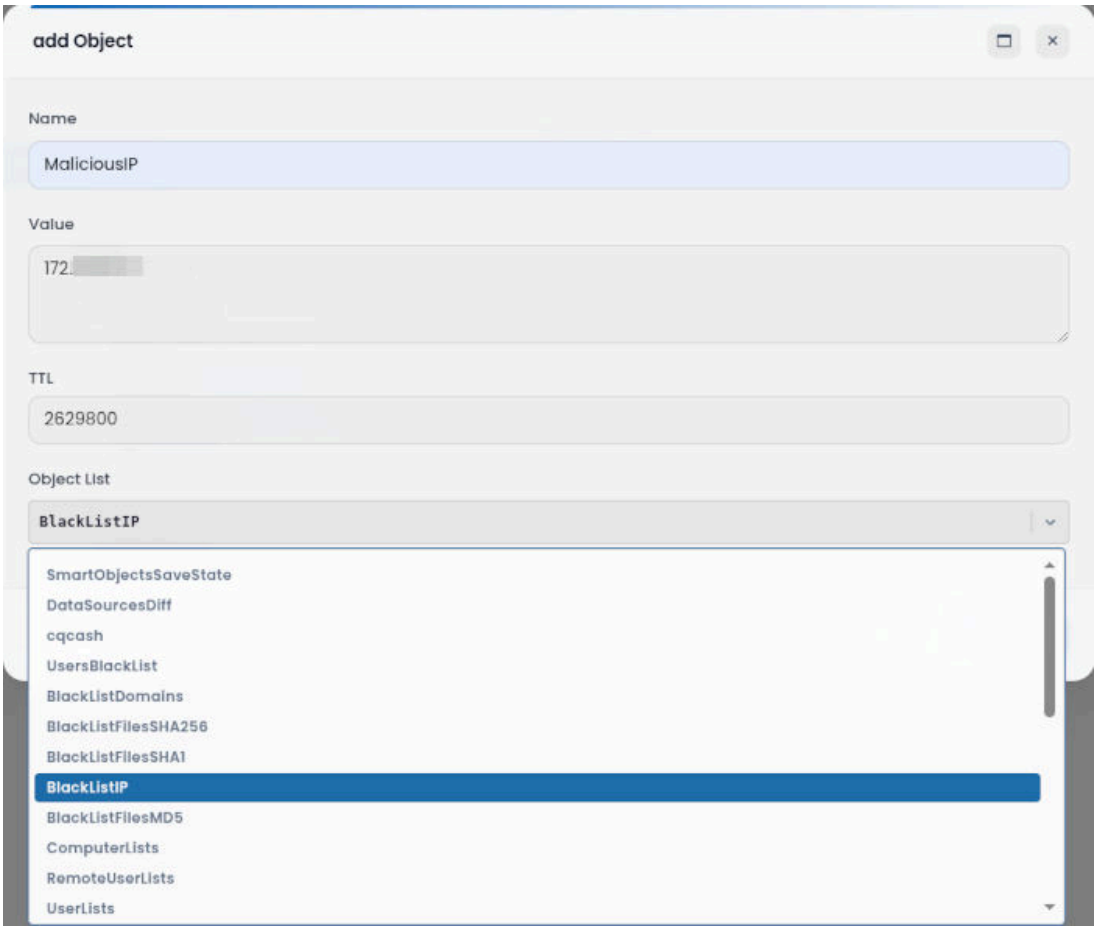
to remove an object. A confirmation prompt ensures objects aren't deleted accidentally.

Creating New Objects

Click the create button



from the Objects management page, the **Add Object** configuration will open:



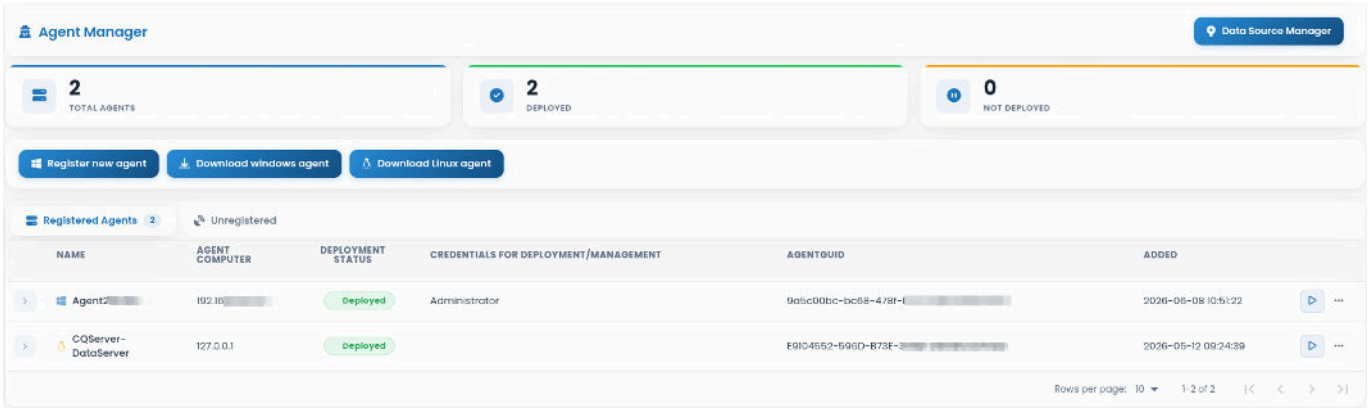
- **Name**: Descriptive name for the object
- **Value**: Specific identifier or value for the object
- **TTL**: Specifies the duration (in seconds) that the object will remain active in the list before it automatically expires and is removed. Entering `-1` will make the object permanent.
- **Object List**: Selects the target list where the object will be added. Examples include `BlackListIP` for blocking IP addresses.

Click “Save” to persist your configuration or “Cancel” to discard changes.

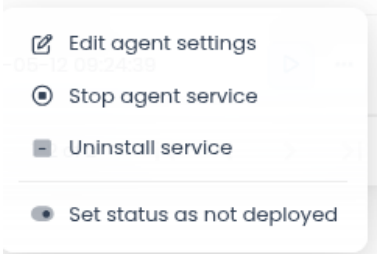
Agent Manager

The Agent Manager in CYBERQUEST provides centralized control over all deployed agents, allowing administrators to register, configure, monitor, and manage agents that collect and forward data from various sources.

Navigate to **Settings > Management > Agent Manager** in the Web Interface to access the agent management page. This interface displays all registered agents and their current status.



Click the **actions menu** next to the agent to access the available management options:



- **Edit agent settings** - Opens the agent configuration window, allowing users to modify the agent's parameters.
- **Stop Agent Service** - Stops the agent service on the target machine.
- **Uninstall Service** - Removes the agent service from the target machine.
- **Set status as not deployed** - Changes the agent status to **Not Deployed**, indicating that the agent is no longer considered deployed in the system.
- **Start Agent Service**

  - Starts the agent service on the target machine. This option is available when the agent service is stopped or not running.
- **Manually Deploy** - Indicates that the agent requires manual deployment or manual intervention before it can be used.
- **Not Deployed** - Indicates that the agent is not currently deployed on the target machine.
- **DOWNLOAD WINDOWS AGENT** - download the latest version of the CYBERQUEST agent. The agent must be installed on a Windows target machine and the file will be downloaded as "*AgentSetup.msi*".

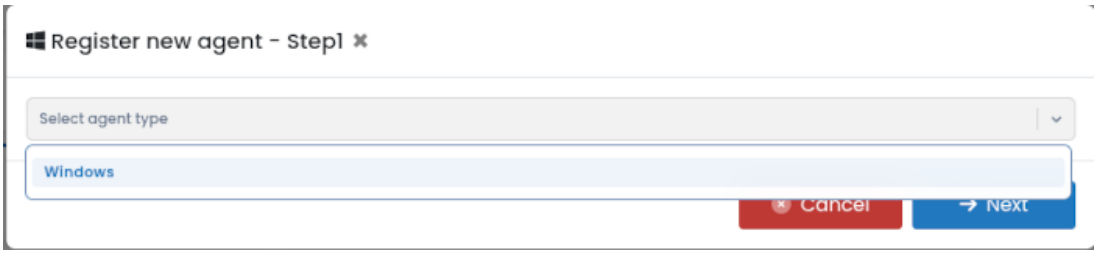
Registering New Agents

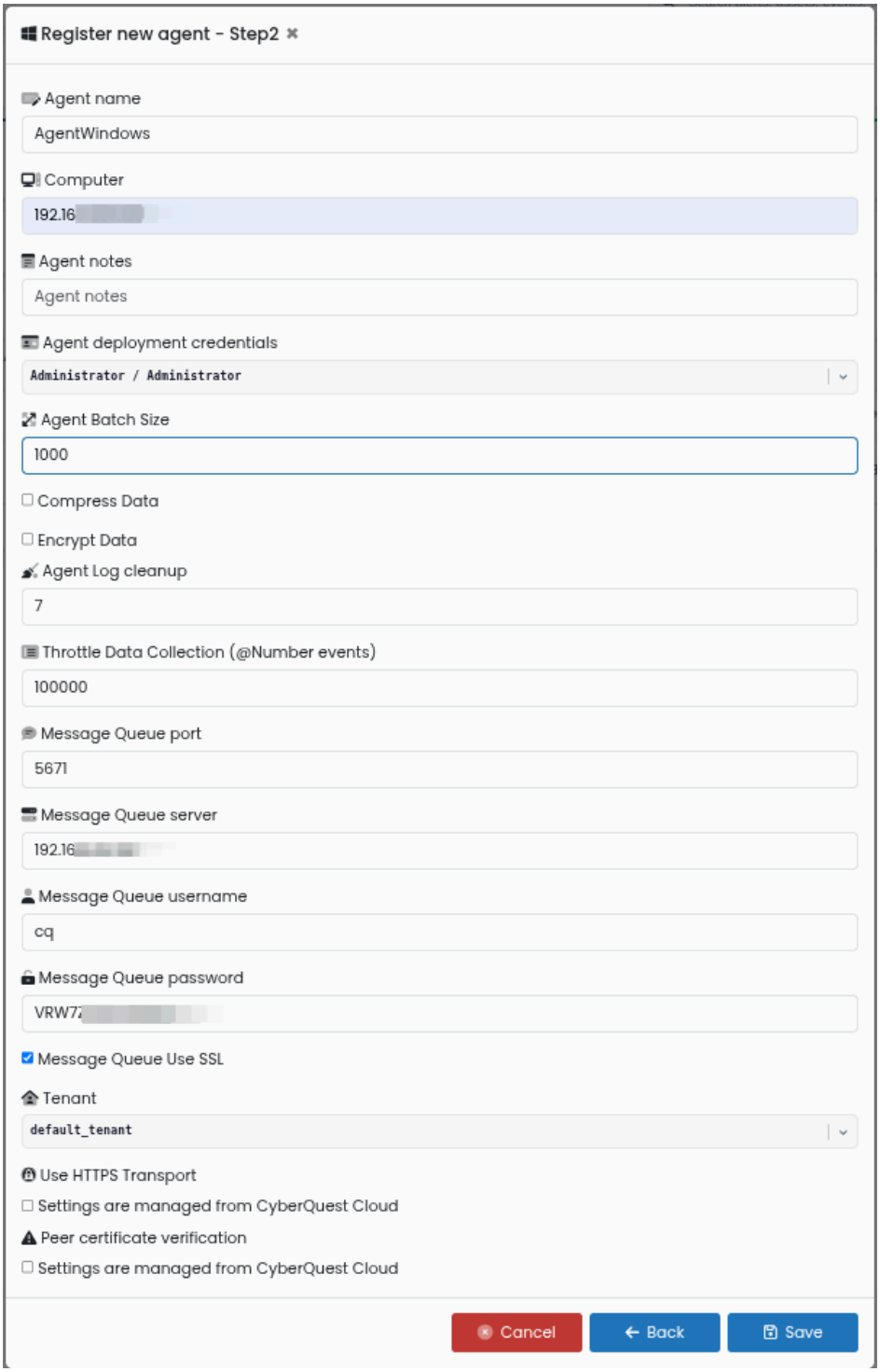
- Click the "Register New Agent" button

  from the Agent Manager page

- Select "Windows" as the target platform and click "Next"
- Complete the agent configuration form with required details





Agent Configuration Parameters

When registering a new agent, several fields must be completed:

- **Agent Name**: The name assigned to the agent for identification within the system.
- **Computer**: The IP address of the host machine where the agent will be installed.
- **Agent Deployment Credentials**: Credentials used for deploying the agent.
- **Tenant**: Choose the appropriate tenant from the available list.
- **Agent Notes**: Optional comments or descriptions for reference
- **Agent Batch Size**: Number of events processed in a single batch
- **Compress Data**: Enable data compression before transmission
- **Encrypt Data**: Enable encryption for secure data transfer
- **Agent Log Cleanup**: Specify log retention and cleanup rules
- **Throttle Data Collection (@Number events)**: Limit event collection rate to prevent system overload

- **Message Queue Port**: Port for message queue communication
- **Message Queue Server**: Hostname or IP of message queue server
- **Message Queue Username**: Authentication username for message queue
- **Message Queue Password**: Password for message queue access
- **Message Queue Use SSL**: Enable SSL for secure queue communication
- **Settings Managed from CyberQuest Cloud**: Allows remote configuration via CyberQuest Cloud

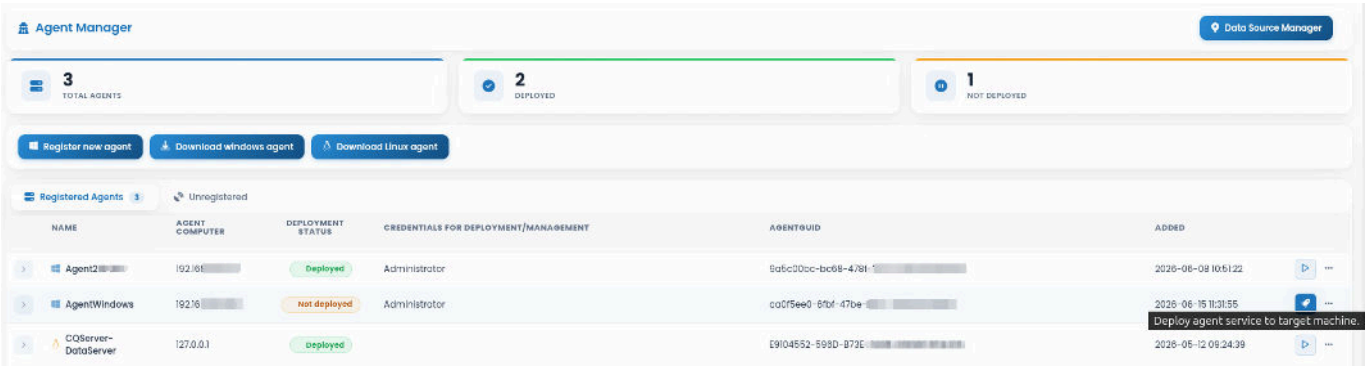
Before starting the "Deploy Agent Service to Target Machine" process, run the following command on the Windows machine using Windows PowerShell. This step creates a required firewall rule to ensure proper communication during the deployment.

```
New-NetFirewallRule -DisplayName "CQ-Agent" -Direction Inbound -LocalPort 445 -Protocol TCP -Action Allow -RemoteAddr
ess "CQ-Address-IP" -Profile Any
```

Once the configuration is saved, the installation process for the Windows agent can begin. To start the deployment, click the



button labeled "Deploy agent service to target machine". This action will initiate the installation of the agent on the specified host using the previously defined settings. Ensure that the target machine is accessible and the deployment credentials are correct before proceeding.



A status message will appear at the top of the screen once the agent installation begins. Wait until the message is displayed - this confirms that the agent has been installed successfully on the target machine.

For detailed instructions on agent deployment and management, refer to:

- Collecting with CQ Windows agent
- How to manually deploy the agent

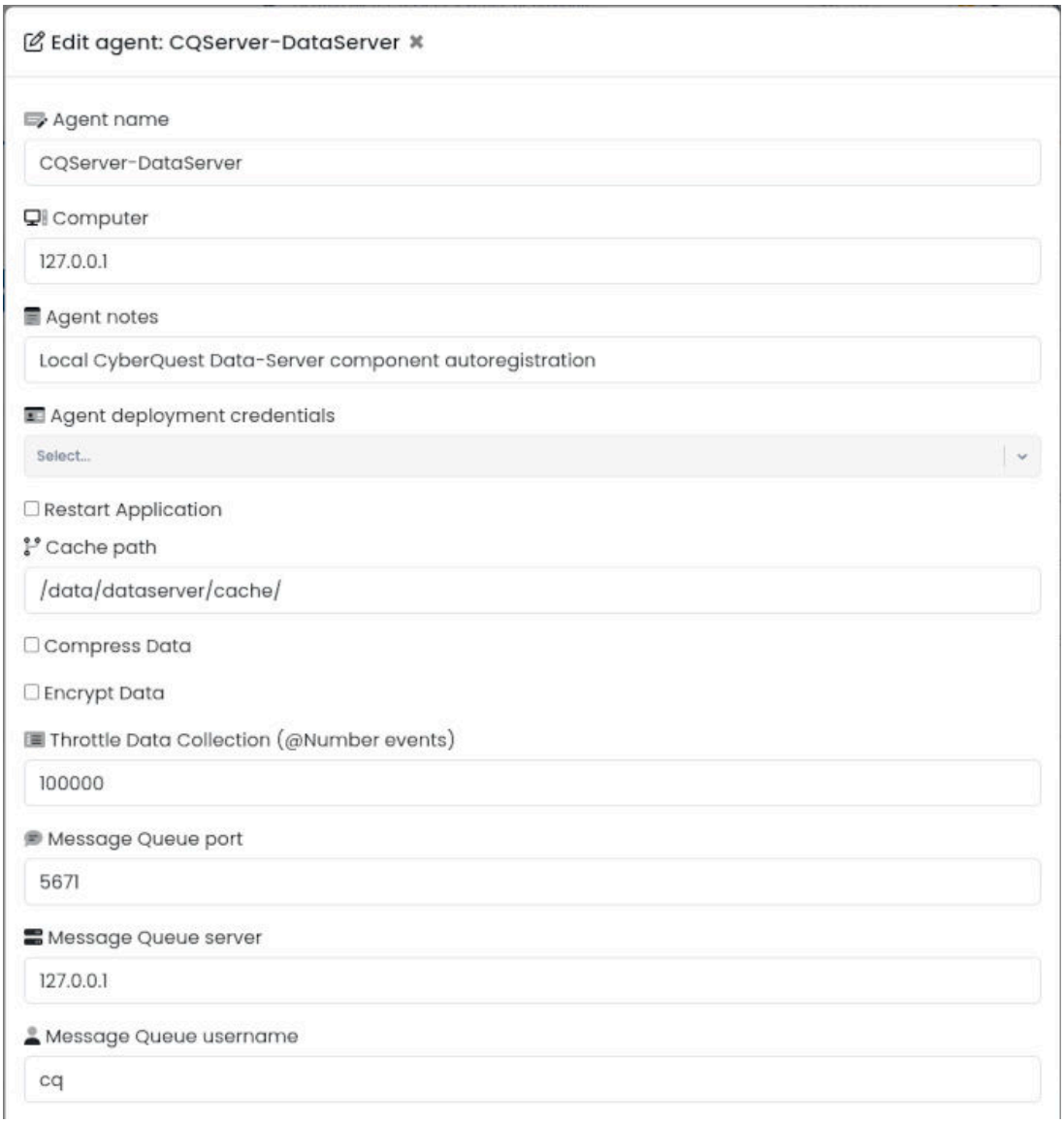
Configuring SNMP Trap collection

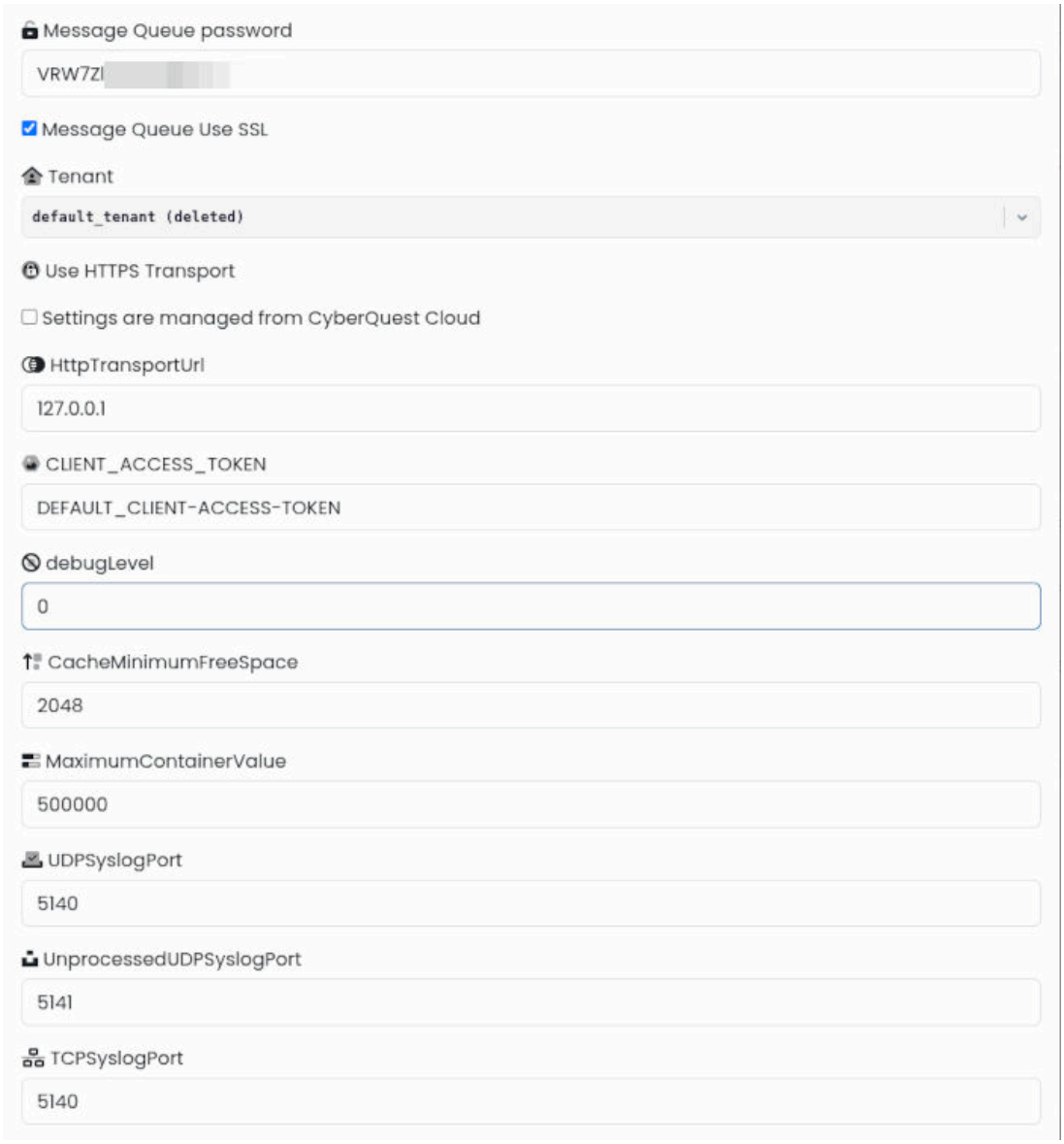
The CYBERQUEST Data Server can be configured to passively receive SNMP Trap messages directly from monitored devices. The platform supports SNMPv1, SNMPv2c and SNMPv3 and includes a library of **388 MIB files** for interpreting and enriching received Trap messages. SNMP Trap reception is configured from **Settings > Management > Agent Manager** by editing the `CQServer-DataServer` agent.

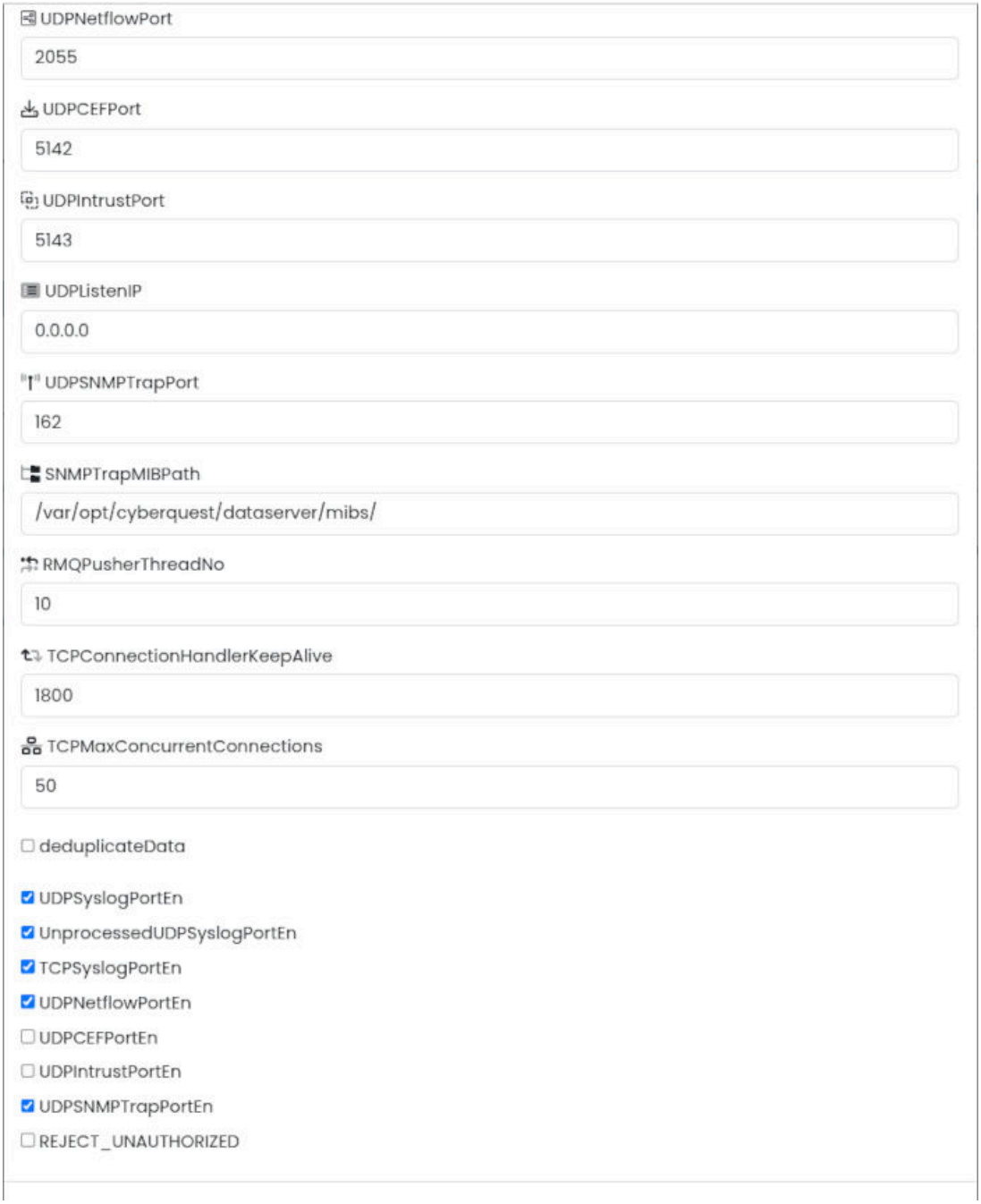
The following parameters are available for SNMP Trap collection:

- **UDPListenIP** - specifies the IP address on which the Data Server listens for incoming UDP traffic. A value of `0.0.0.0` enables listening on all available network interfaces.
- **UDPSNMPTrapPort** - specifies the UDP port used for receiving SNMP Trap messages. The default SNMP Trap port is `162`.
- **SNMPTrapMIBPath** - specifies the location of the MIB files used when processing SNMP Trap messages. CYBERQUEST includes a library of **388 MIB files**, which can be used to interpret and enrich received SNMP Trap messages with vendor- and device-specific information.
- **UDPSNMPTrapPortEn** - enables or disables the SNMP Trap listener.

When SNMP Trap collection is enabled, CYBERQUEST can receive and process SNMPv1, SNMPv2c and SNMPv3 Trap messages transmitted by network devices.




Message Queue password
VRW7Zl
Message Queue Use SSL
Tenant
default_tenant (deleted)
Use HTTPS Transport
Settings are managed from CyberQuest Cloud
HttpTransportUrl
127.0.0.1
CLIENT_ACCESS_TOKEN
DEFAULT_CLIENT-ACCESS-TOKEN
debugLevel
0
CacheMinimumFreeSpace
2048
MaximumContainerValue
500000
UDPSyslogPort
5140
UnprocessedUDPSyslogPort
5141
TCPSyslogPort
5140



Linux Agent

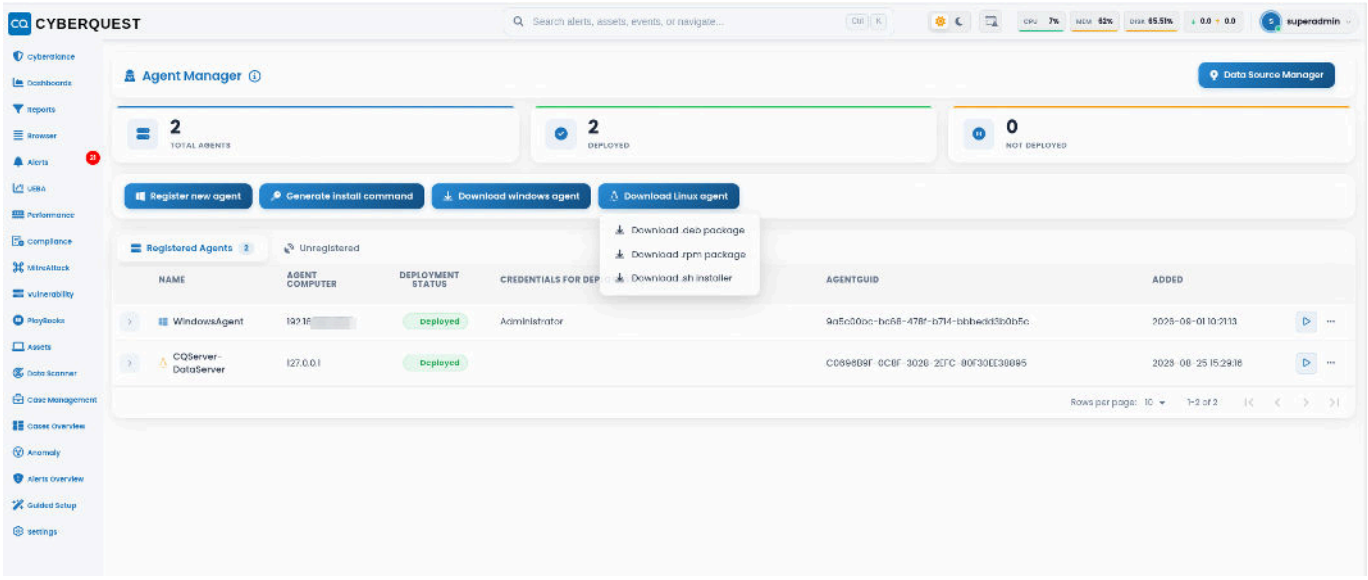
The **CYBERQUEST Linux Agent** provides native security event collection and file monitoring for Linux systems. It monitors security-relevant operating system resources, generates normalized CYBERQUEST events when monitored files are created, modified, or deleted, and securely forwards collected events to the CYBERQUEST platform.

The Linux Agent can also process Syslog events received through the CYBERQUEST Data Server, applying the required normalization and enrichment before the events enter the CYBERQUEST processing and correlation pipeline.

Installation packages

The Linux Agent can be downloaded directly from **Agent Manager**. CYBERQUEST provides:

- `.deb` package for Debian/Ubuntu-based distributions
- `.rpm` package for RPM-based distributions
- `.sh` installer



Installing the Linux Agent

For Debian/Ubuntu-based systems:

```
sudo dpkg -i ./CQLinuxAgent.deb
```

During installation, the installer displays the CYBERQUEST Linux Agent EULA and generates a unique Agent GUID. The Configuration Server URL is then specified to establish the connection with the CYBERQUEST platform.

After successful installation, the agent is registered as the `CQLinuxAgent.service` systemd service.

The configuration file is located at:

```
/var/opt/cyberquest/linux_agent/linux-agent.env
```

Service management

Start the Linux Agent:

```
sudo systemctl start CQLinuxAgent.service
```

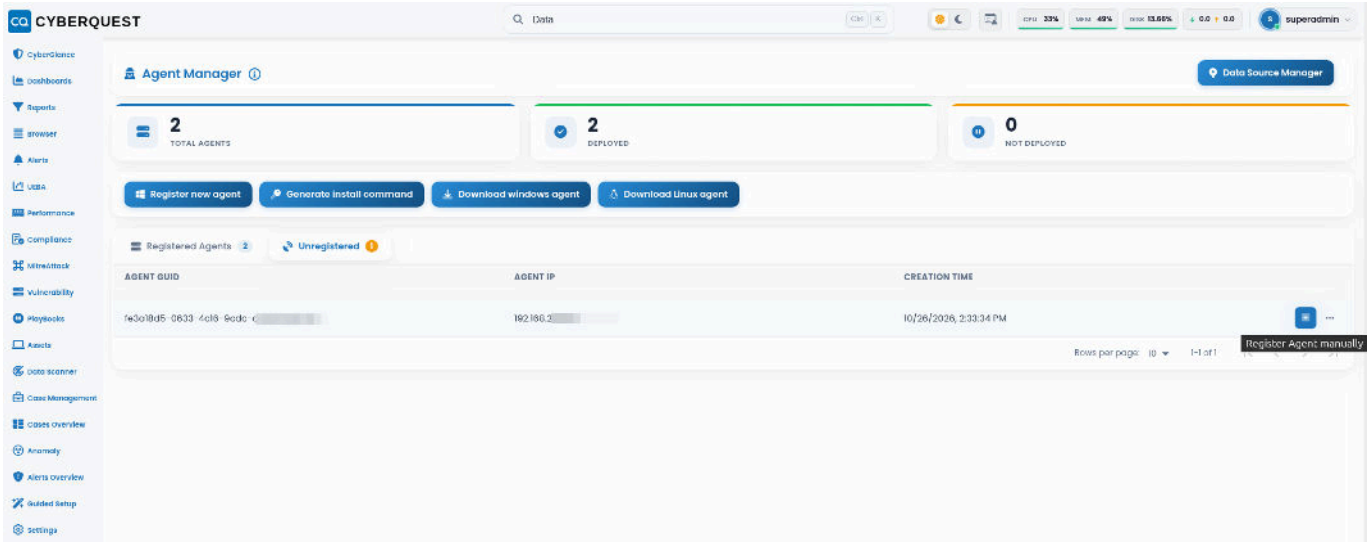
Check the service status:

```
sudo systemctl status CQLinuxAgent.service
```

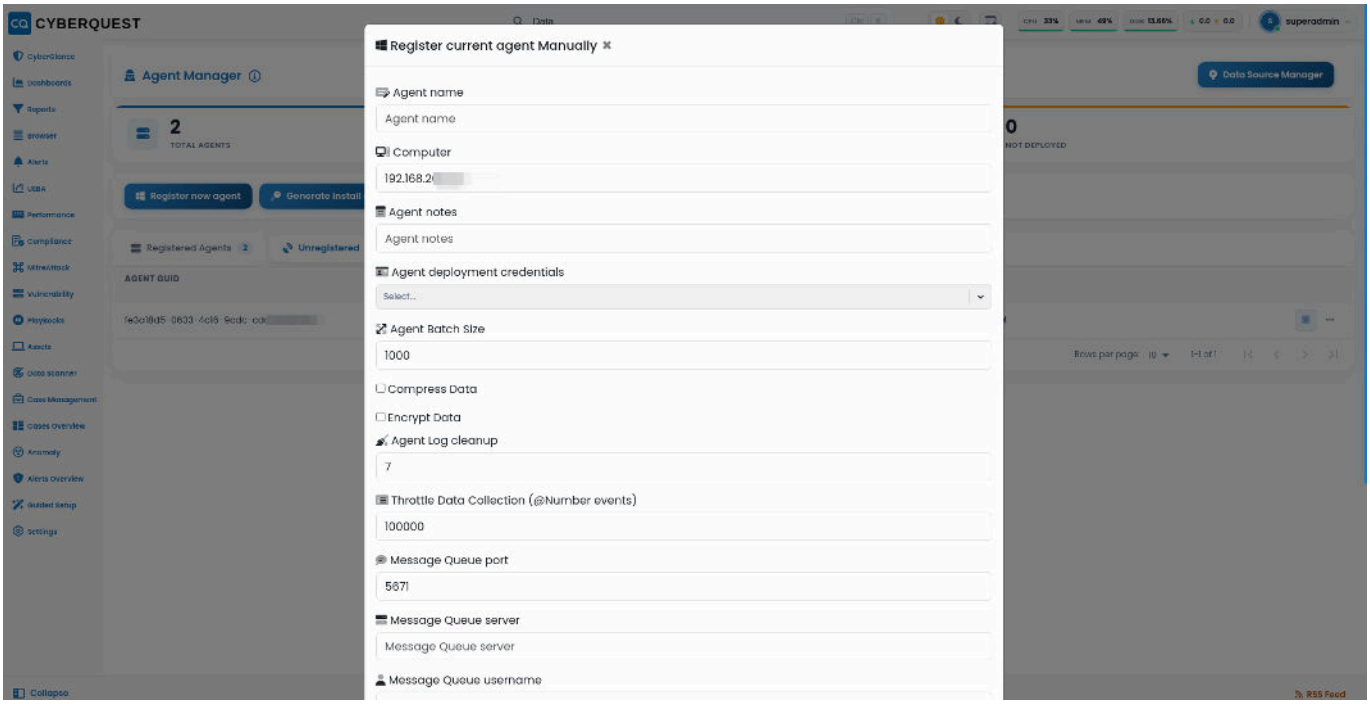
Registering and configuring the Linux Agent

After starting the Linux Agent service, open the CYBERQUEST Web Interface and navigate to **Settings > Management > Agent Manager** to register and configure the agent.

Select the **Unregistered** tab and locate the Linux Agent by its **Agent GUID** or **Agent IP**. Click the **Register Agent manually** button (**+**) next to the agent to open the registration form.

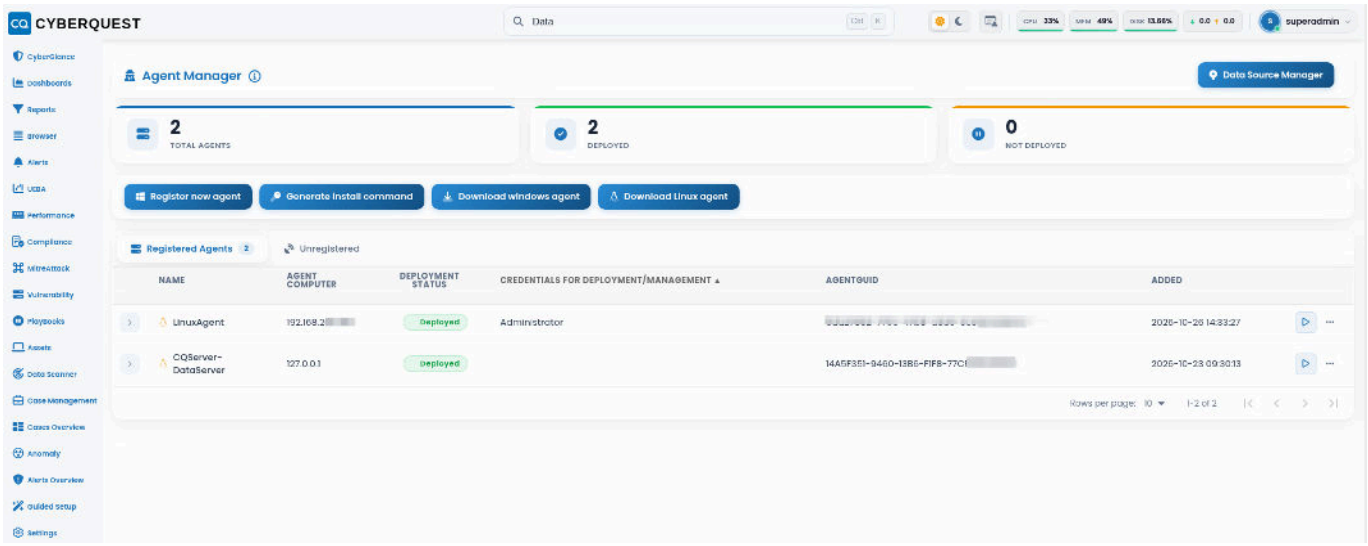


In the **Register current agent Manually** window, complete the agent configuration:



- **Agent name** - Enter a descriptive name to identify the agent in CYBERQUEST.
- **Computer** - Verify that the prefilled IP address matches the Linux host where the agent is installed.
- **Agent notes** - Add optional notes about the agent or the monitored host.
- **Agent deployment credentials** - Select the appropriate credentials if required for your deployment.
- **Agent Batch Size** - Specify the number of events processed in a single batch.
- **Compress Data** - Enable data compression before transmission, if required.
- **Encrypt Data** - Enable data encryption, if required.
- **Agent Log cleanup** - Configure the agent log cleanup settings.
- **Throttle Data Collection (@Number events)** - Set the event collection limit.
- **Message Queue port** - Enter the port used to connect to the message queue server.
- **Message Queue server** - Enter the hostname or IP address of the message queue server.
- **Message Queue username** - Enter the username used to authenticate to the message queue server.
- **Message Queue password** - Enter the password associated with the message queue username.
- **Tenant** - Select the appropriate tenant from the drop-down list.

Save the configuration to complete the registration. Open the **Registered Agents** tab and verify that the Linux Agent is listed. Review its **Deployment Status** and use the actions menu next to the agent to access its configuration and management options.



View agent logs:

```
journalctl -u CQLinuxAgent.service
```

Monitor logs continuously:

```
journalctl -u CQLinuxAgent.service -f
```

File-system security monitoring

The CYBERQUEST Linux Agent provides native monitoring of security-sensitive Linux files and directories. Changes to monitored objects are converted into dedicated CYBERQUEST security events.

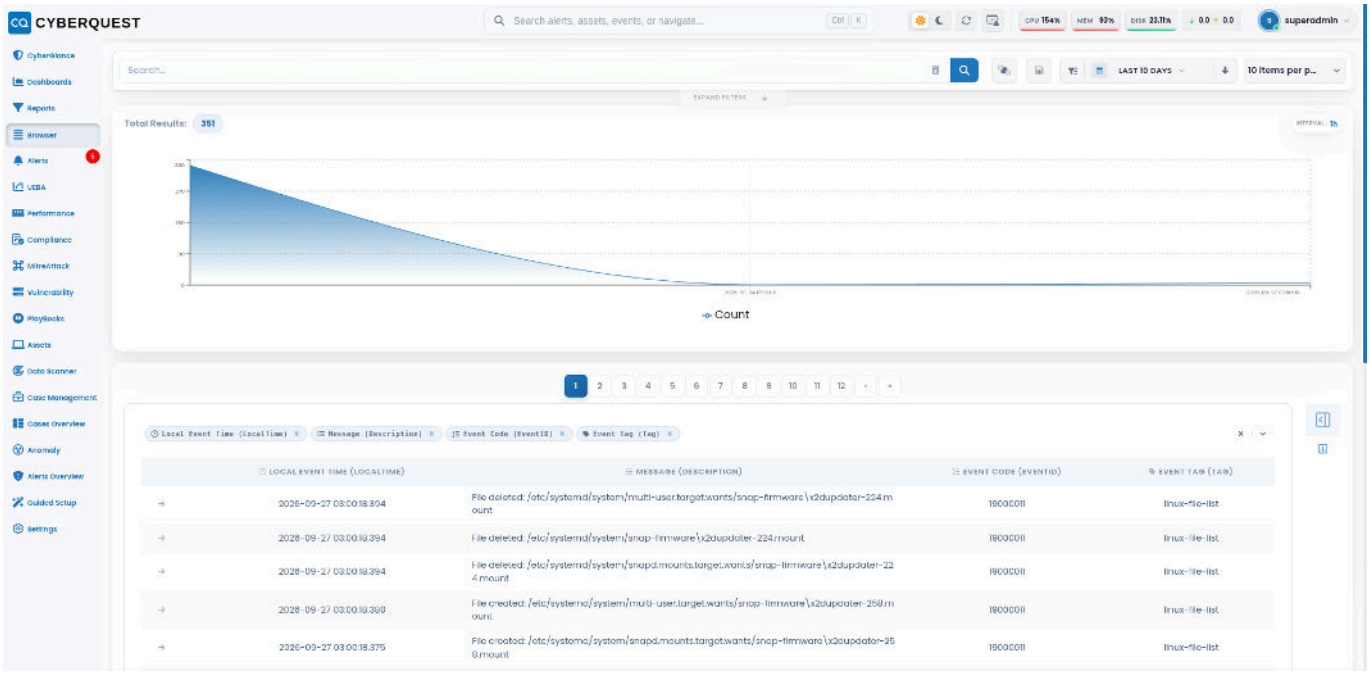
The agent detects **file creation, modification, and deletion** and records contextual information including:

file path, change type, file size, last-write time, Unix mode, file attributes, owner UID/GID, permissions, previous size, previous owner and previous permissions.

Monitored security-sensitive resources include, among others:

`/etc/shadow`, `/etc/passwd`, `/etc/group`, `/etc/gshadow`, `/etc/sudoers`, `/etc/sudoers.d/*`, user `.ssh/authorized_keys`, `/etc/crontab`, `/etc/cron.d/*`, `/var/spool/cron/crontabs/*`, `/etc/systemd/system/*`, `/etc/ld.so.preload`, user `.bashrc`, `/etc/hosts`, `/etc/resolv.conf` and `/etc/ssh/sshd_config`.

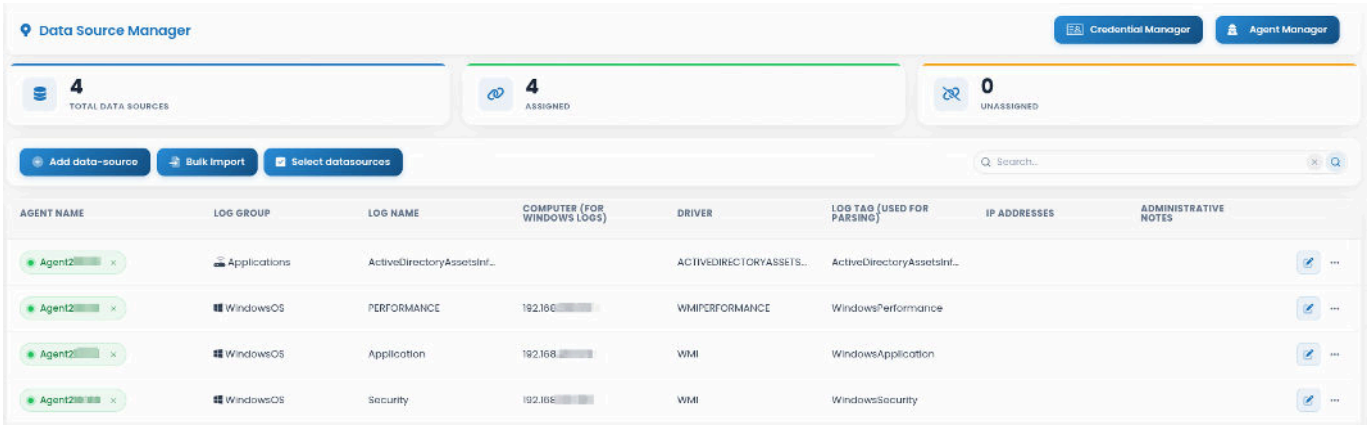
The agent also monitors security-relevant Linux log files such as `/var/log/auth.log`, `/var/log/secure` and `/var/log/audit/audit.log`.



Data Source Manager

A centralized tool in CYBERQUEST for managing all data sources. It allows administrators to configure, monitor, and maintain the systems, applications, and services that provide security events, logs, and telemetry for analysis.

Navigate to **Settings > Management > Data Sources Manager** in the Web Interface to access the data source management page. This interface displays all configured data sources and their current status.



- **Bulk Clone**



: Clone the current data source settings for multiple elements specified in the “Bulk Clone” field. Useful for creating similar configurations across multiple systems or data sources.

- **Clone**



: Duplicate an existing data source configuration. The copy starts with the same settings and can be adjusted as needed.

- **Edit**



: Modify data source configuration parameters, including collection settings, parsing rules, and integration options.

- **Delete**



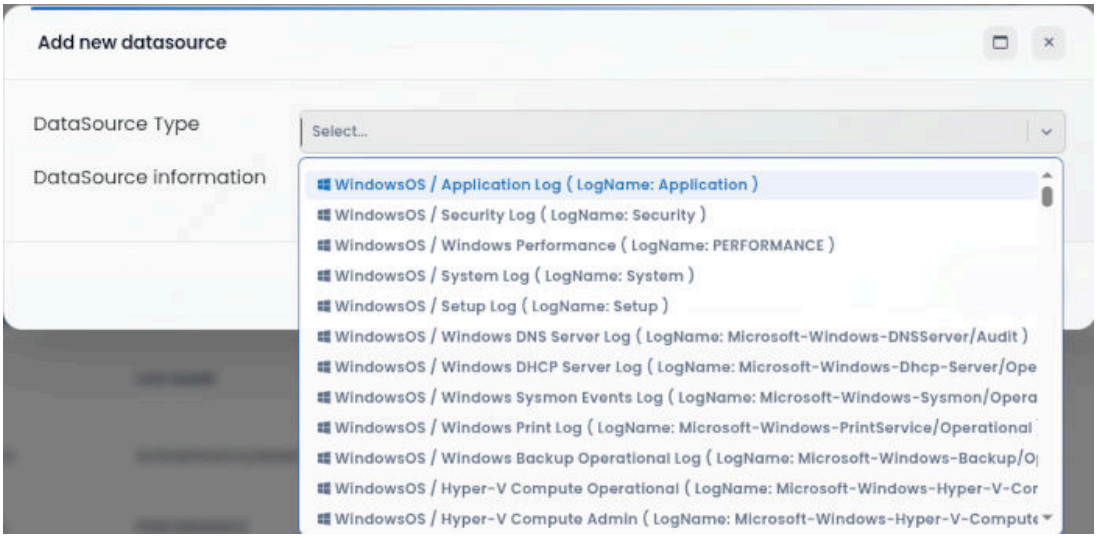
: Remove a data source from the system. Requires confirmation to prevent accidental deletion.

Adding New Data Sources

- To add a new data source click the “Add Data Source” button



and a selection window will open presenting available data source types from a predefined list.



- Complete the configuration form with required details specific to the data source type.
- Click “Save” to persist your configuration or “Cancel” to discard changes.

The **Select datasource** button



reveals a comprehensive menu for managing multiple data sources simultaneously:



- **Assign Agent**: Assign multiple agents to selected data sources. Use the checkboxes to select the data sources, then choose the agent that will collect and forward data to CYBERQUEST.
- **Unassign Agents**: Remove agent assignments from multiple data sources. This stops data collection from the selected sources until new agents are assigned.
- **Bulk delete**: Delete multiple data sources in a single operation. Useful for cleaning up obsolete or unused data sources.
- **Close selection**: Close the bulk operations menu and return to standard view.
- **Bulk Export** : Export multiple selected data sources at once. The exported file contains their configurations, which can be saved for backup or reused later.

For detailed instructions on configuring specific data source types, refer to:

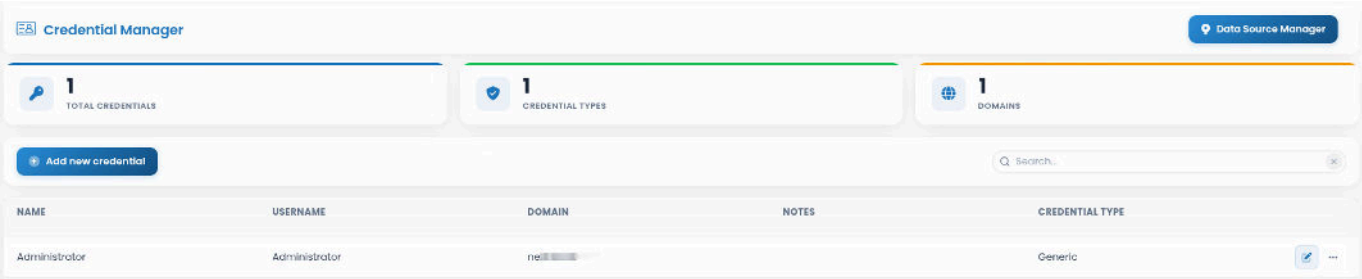
- How to collect data from Check Point Firewall
- How to collect data on Active Directory
- How to collect data on Windows Application Log
- How to collect data on Windows Security Log
- How to collect data on Windows System Log
- How to connect to CQ Threat Intelligence

- How to connect to Active Directory

Credential Manager

Credential Manager - Safely stores and manages the credentials used by agents and data sources. All credentials are encrypted, accessed only by authorized components, and managed from a single, central interface.

Navigate to **Settings > Management > Credential Manager** in the Web Interface to access the credential management page. This interface displays all stored credentials and provides tools for managing them.



- Click edit button

  to modify the properties of an existing credential. Passwords must be re-entered, and changes take effect immediately for all agents using it.
- Click edit button

  to permanently remove a credential after confirmation. Make sure it's not in use by any active agents or data sources.

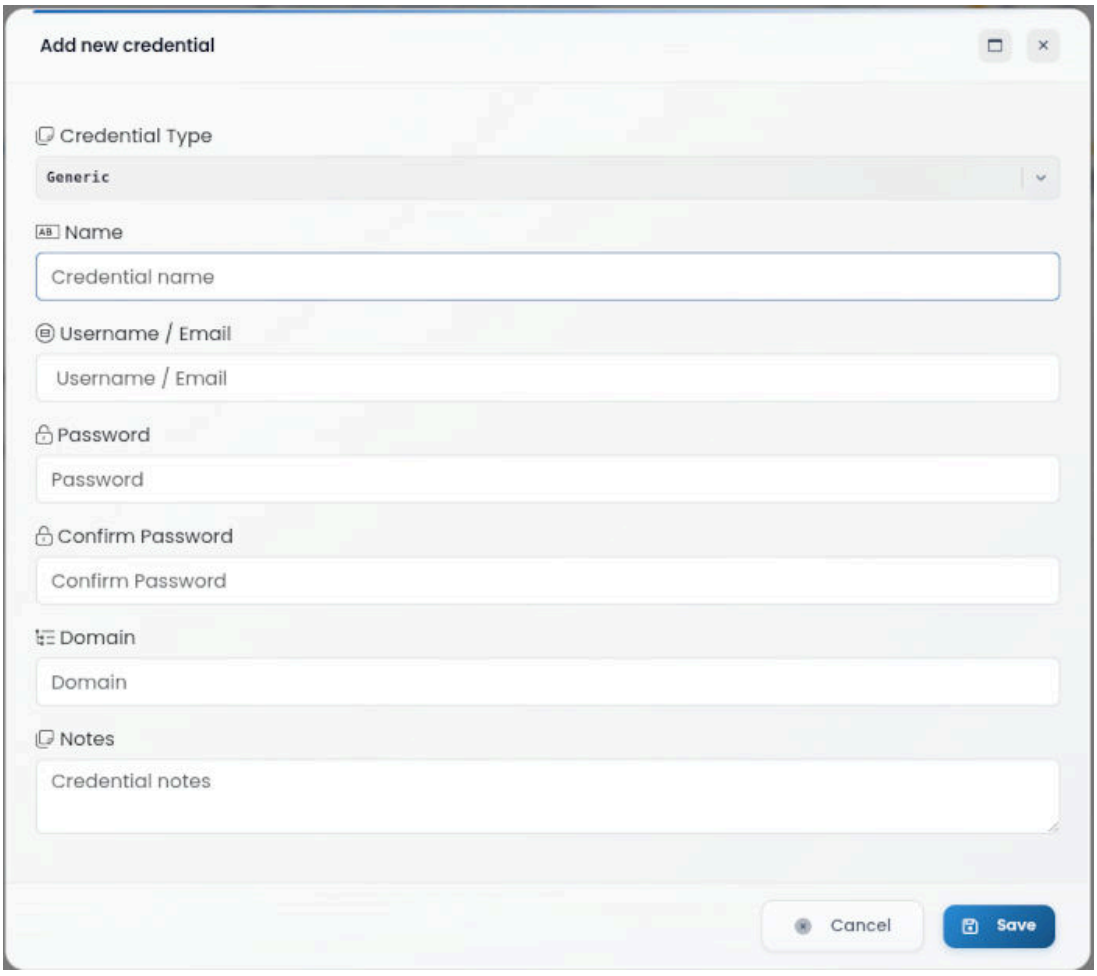
Creating New Credentials

To create a new credential set:

- Click the "Add Credential" button

- The credential configuration form will open:



Complete the form with the following parameters:

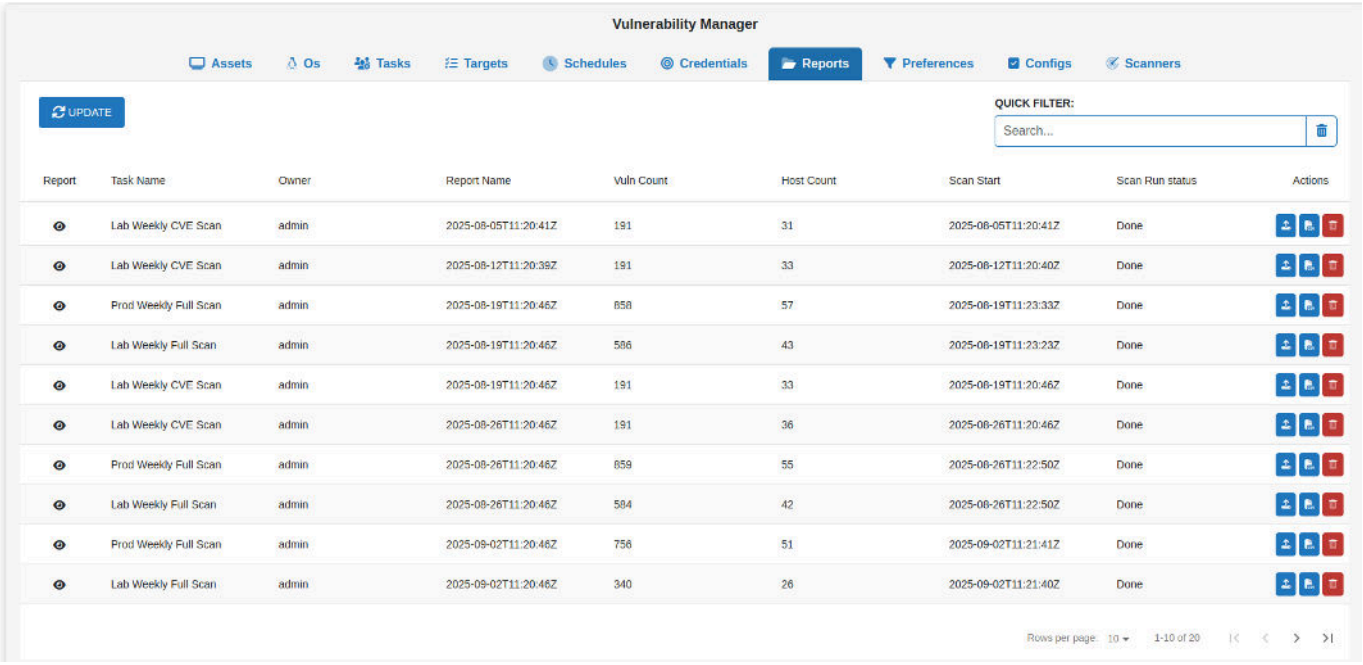
- **Credentials Type**: Select the type of credential:
  - **Generic (default)** - Standard username/password credentials.
  - **APIKey** - Access key for API authentication.
  - **SSHPublicKey** - SSH public key for secure login.
  - **Token** - Authentication token for services.
  - **APIKeyWithPassword** - API key that also requires a password.
- **Name:** A clear, descriptive name for the credential set that shows its purpose and associated system.
- **Username/Email:** The username or email address used for authentication. For system accounts, use the full username format (e.g., "DOMAIN\username").
- **Password:** The password for the account. Make sure it is strong and secure.
- **Confirmation Password:** Re-enter the password to confirm accuracy.
- **Domain:** The domain name for domain user credentials. Leave blank for local accounts.
- **Notes:** Optional comments or descriptions about the credential's usage, purpose, or restrictions.

Click "Save" to store the credentials or "Cancel" to discard changes.

Vulnerability Manager

Vulnerability Assessment Module - Uses OpenVAS (https://www.openvas.org/) to provide full-featured vulnerability scanning for systems.

Navigate to **Settings > Management > Vulnerability Manager** in the Web Interface to access the vulnerability management dashboard. This interface provides centralized control over vulnerability scanning operations, results, and remediation tracking.



For detailed information about vulnerability management capabilities, refer to: Vulnerability Manager

Tag Alias

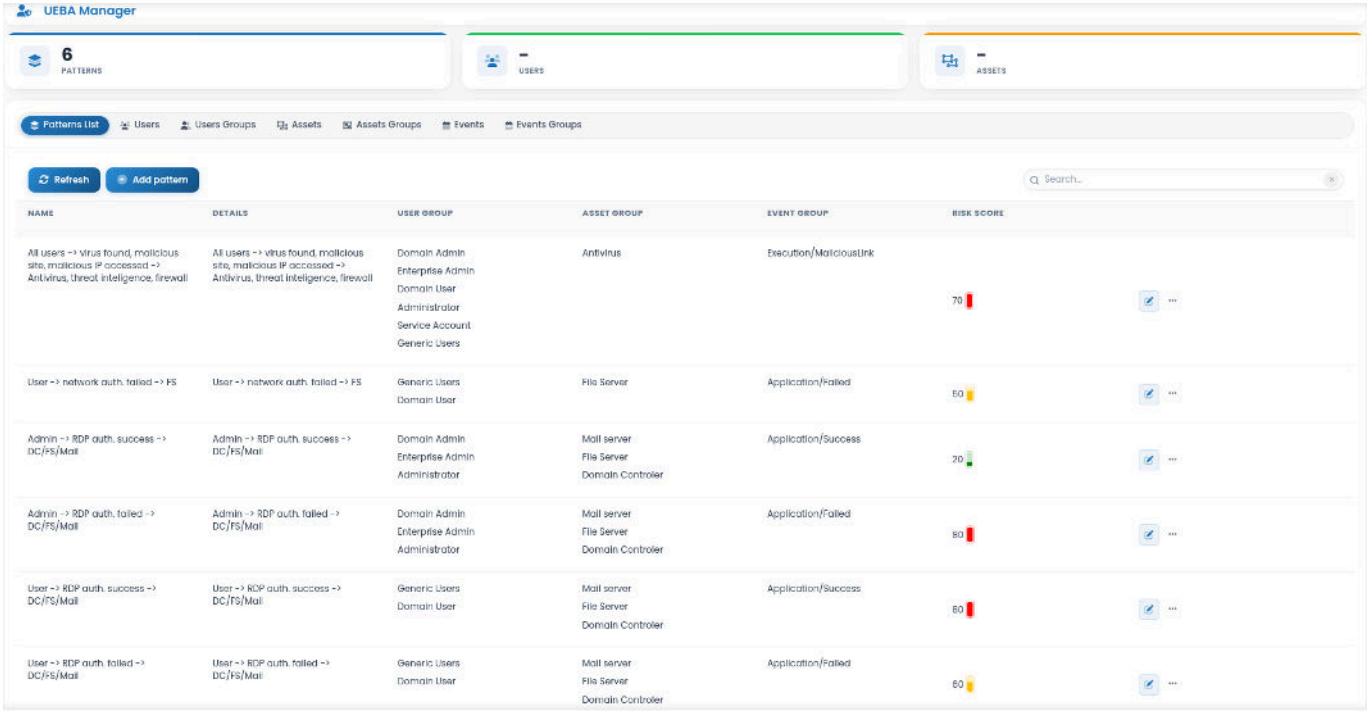
Tag Alias - Enables events from a data source to be processed with a different parser than the one originally assigned. This allows better handling of misclassified events, improved parsing, or customized processing without changing the original event definitions.

For detailed information about Tag Alias functionality and advanced configuration, refer to: Tag Alias

UEBA Manager

UEBA Manager helps organizations detect and respond to potential security threats more effectively, reducing the risk of data breaches and insider misuse while strengthening overall security. It identifies unusual user behavior, such as accessing data outside normal hours, connecting from unfamiliar locations, or downloading large amounts of information. By recognizing these patterns, **UEBA Manager** enables quick detection and response to suspicious activities.

Navigate to **Settings > Management > UEBA Manager** in the Web Interface to access the UEBA management dashboard. This interface provides centralized control over behavioral analytics configurations, group memberships, and monitoring settings.



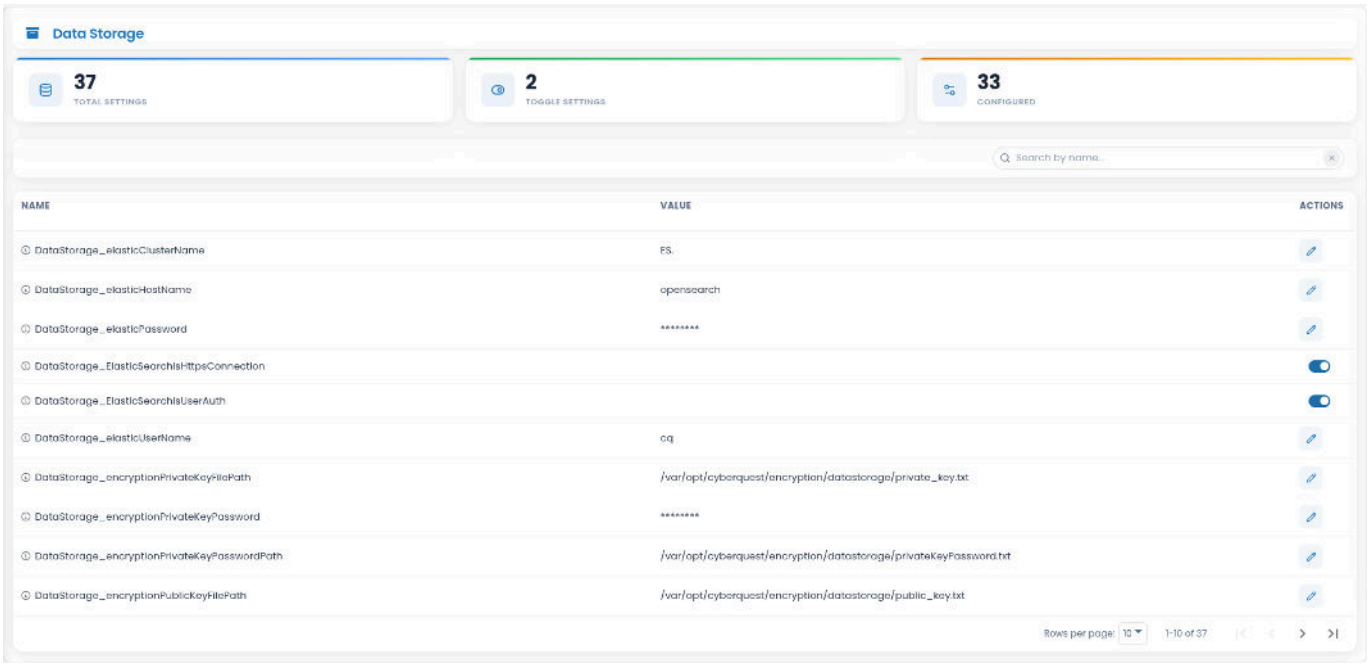
For detailed information about UEBA capabilities and advanced configuration, refer to: How to manage UEBA

Data Storages

Data Storage Management provides centralized control for managing how data is collected, processed, and stored in CYBERQUEST. Administrators can configure storage settings, message queues, encryption options, and integrations with external systems such as Elasticsearch.

Navigate to **Settings > Application Settings > Data Storage** in the Web Interface to access the data storage configuration page. This interface provides a user-friendly way to configure storage parameters without directly editing configuration files.

The Data Storage configuration page displays all configurable parameters:



Data Storage Configuration enables advanced setup of data storage components used by CYBERQUEST. To modify the configuration, open the `/var/opt/cyberquest/datastorage/conf.xml` file on the CYBERQUEST server.

All configurable parameters are listed in the table below:

Parameter	Description	Default Value
dbDriver	JDBC driver class for MySQL database	com.mysql.jdbc.Driver
dbUserName	Database username for configuration access	root
dbPass	Database password for configuration access	****
dbUrl	JDBC connection URL for primary database	jdbc:mysql://127.0.0.1:3306/config
dbAlternateUrl	JDBC connection URL for failover database	jdbc:mysql://127.0.0.1:3306/config
serverGuid	Unique identifier for the server instance	D39498A9-1C85-0379-1E78-C161E6FFEEEA

To modify a variable, click the **Edit** button. After making changes, click **Save** to apply them or **Cancel** to discard them.

All configurable variables are listed in the table below.

Parameter	Description	Default Value
maxEventsPerFile	Maximum events per storage file	20000
fileWriterTimeout	Timeout for event writer operations (seconds)	60
mqUserName	Username for MQ service authentication	cq
mqPassword	Password for MQ service authentication	****
mqHost	Hostname or IP address of MQ server	127.0.0.1
mqVhost	The MQ service virtual server. In distributed architectures, it may differ from the default CYBERQUEST server	/
mqPort	Network port for MQ communication	5672
mqExchangeName	Default exchange name for event processing	eventsExchange
mqQueueName	The MQ queue name	jobCommands
mqReceiveQueueType	The MQ Receive queue type	fanout
mqRouting	The routing path for message queues	agents
mqReceiveCommandExchangeName	The MQ Receive command exchange name	eventsExchange
mqReceiveCommandQueueName	Specifies the MQ Receive command queue name	jobCommands
mqReceiveCommandQueueType	Specifies the MQ Receive command queue type	direct
mqReceiveCommandRouting	Specifies the MQ Receive command routing path	servers

Parameter	Description	Default Value
mqSendExchangeName	The MQ Send exchange name	
mqSendQueueName	Specifies the MQ Send queue name	archive
mqSendRouting	Specifies the MQ Send routing path	agents
mqSendQueueType	Specifies the MQ Send queue type	direct
encryptionPublicKeyFilePath	Path to public key file for encryption	/var/opt/cyberquest/encryption/datastorage/public_key.txt
encryptionPrivateKeyFilePath	Path to private key file for decryption	/var/opt/cyberquest/encryption/datastorage/private_key.txt
elasticClusterName	Online DataStorage cluster name	ES.
elasticHostName	Elasticsearch host address	127.0.0.1
encryptionPrivateKeyPassword	Password for private key encryption	***
encryptionPrivateKeyPasswordPath	Path to file containing private key password	/var/opt/cyberquest/encryption/datastorage/privateKeyPassword.txt
fileImportThreads	How many threads are used for import	5
mqQueueType	Specifies the queue type	direct
mqReceiveExchangeName	Specifies the MQ Receive exchange name	DA.publish
mqReceiveQueueName	The MQ Receive queue name	DataStorage
mqReceiveRouting	Specifies the MQ Receive routing key	agents
mqAlternateHost	The alternate host name to use if the current queue is dead	127.0.0.1
mqVHost	The MQ Receive virtual host	/
elasticUserName	Online DataStorage user name	cq
elasticPassword	Password for Online	***

Parameter	Description	Default Value
	DataStorage authentication	
ElasticSearchIsHttpsConnection	Enable HTTPS for Online DataStorage communication	1
ElasticSearchIsUserAuth	Enable user authentication for Online DataStorage	1

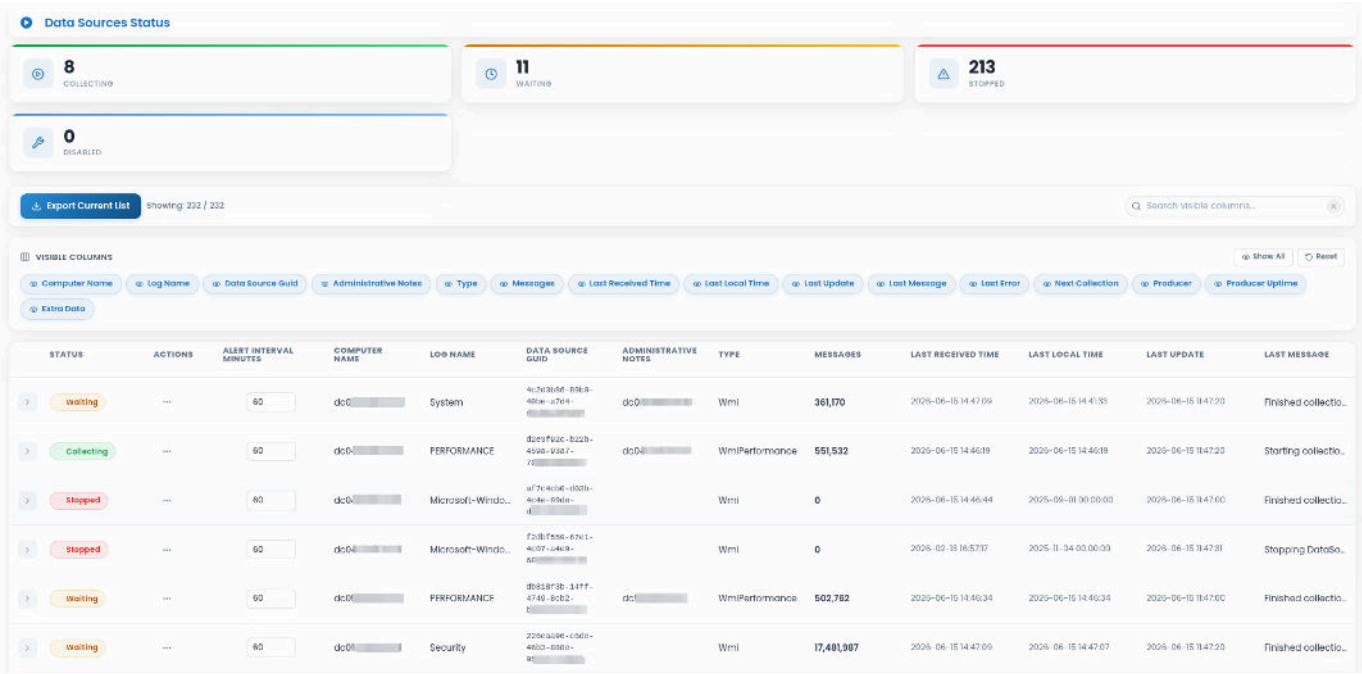
The list below provides examples of defined jobs.

- How to restore data from archive
- How to create a Copy job
- How to create a RTBF job
- How to delete data from Data Storage

Data Sources Status

Data Sources Status - Shows real-time information on the health and performance of all data collection activities. It helps administrators ensure that data sources are actively collecting events, quickly spot any issues, and maintain continuous data flow for monitoring and analysis.

Navigate to **Settings > Management > Data Sources Status** in the Web Interface to access the data source monitoring dashboard. This interface provides a centralized view of all data collection activities.



Data source status is displayed using color-coded indicators for quick visual assessment:

🟢 **Collecting (Green)**: Data source is actively collecting events and forwarding them to CYBERQUEST

🟡 **Waiting for Next Collection (Yellow)**: Scheduled data source awaiting its next collection cycle

🔴 **Stopped or Critical Error (Red)**: Data collection has stopped due to critical error or configuration issue

⚫ **Disabled (Black/Gray)**: Data source has been manually disabled by administrator

An



icon indicates that collection is scheduled to execute at defined time intervals, while sources without this icon execute in real-time.

The list can be sorted by any column or exported by clicking the



button.

Since CYBERQUEST can handle a large number of data collections, the collection status list may become long. Up to 100 entries can be displayed per page. Avoid combining many entries with automatic page refresh to prevent performance issues.

The **Columns** menu at the top of the page allows selection of which columns are shown for all entries. Details for each column are listed in the table below.

Field	Description
Computer Name	Source name (network IP address or resolved FQDN)
Log Name	Name of the log source
Type	Log type category
Messages	Number of collected events
Last Received Time	Last current time when data was received from source
Last Local Time	Last device time when data was received from source
Last Update Time	Last time a modification was made for data source
Last Message	Last message from data collector
Last Error	Last error message from data collector
Next Collection	Date and time when next collection will start
Producer	Module or agent that collected the events
Producer Uptime	Uptime of module or agent that collects events
Extra Data	Additional comments or contextual information
Alert Interval Minutes	Time interval to check source status

Networks

The **Management > Networks** section lets administrators organize and configure network segments across the infrastructure. Networks can be classified by **zone** and **tenant**, which helps improve monitoring accuracy and security scoring.

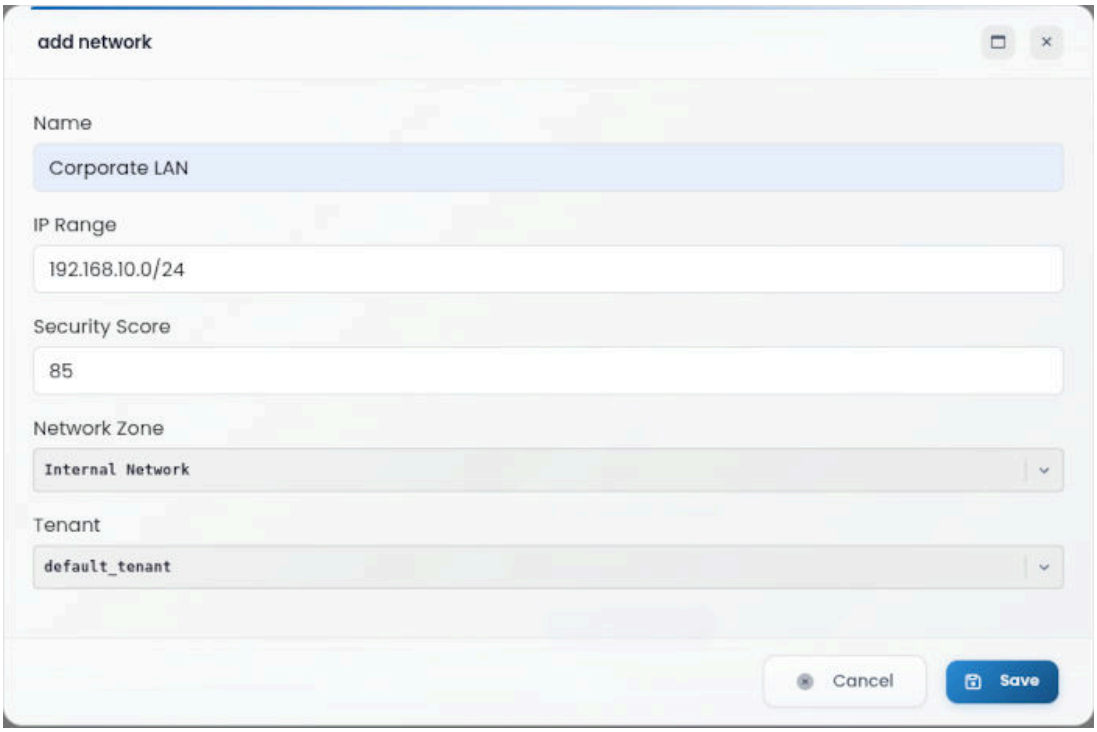
Creating New Network

Click the create button



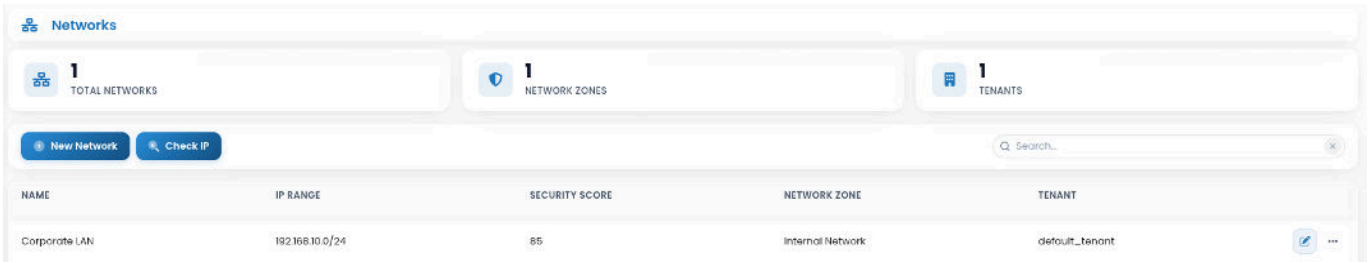
from the Networks management page.

The **Add network** configuration window will open:



- **Name** - a descriptive name for the network segment to easily identify it.
- **IP Range** - the range of IP addresses that belong to this network segment (e.g., 192.168.10.0/24).
- **Security Score** - a numeric value representing the network's security level or risk assessment.
- **Network Zone** - the classification of the network, such as Internal Network, Internal Network, DMZ, Internal Cloud, or External Cloud for better monitoring and policy application.
- **Tenant** - the organizational unit, team, or group responsible for or associated with the network segment.

Once an network is created, the following actions can be performed on it:

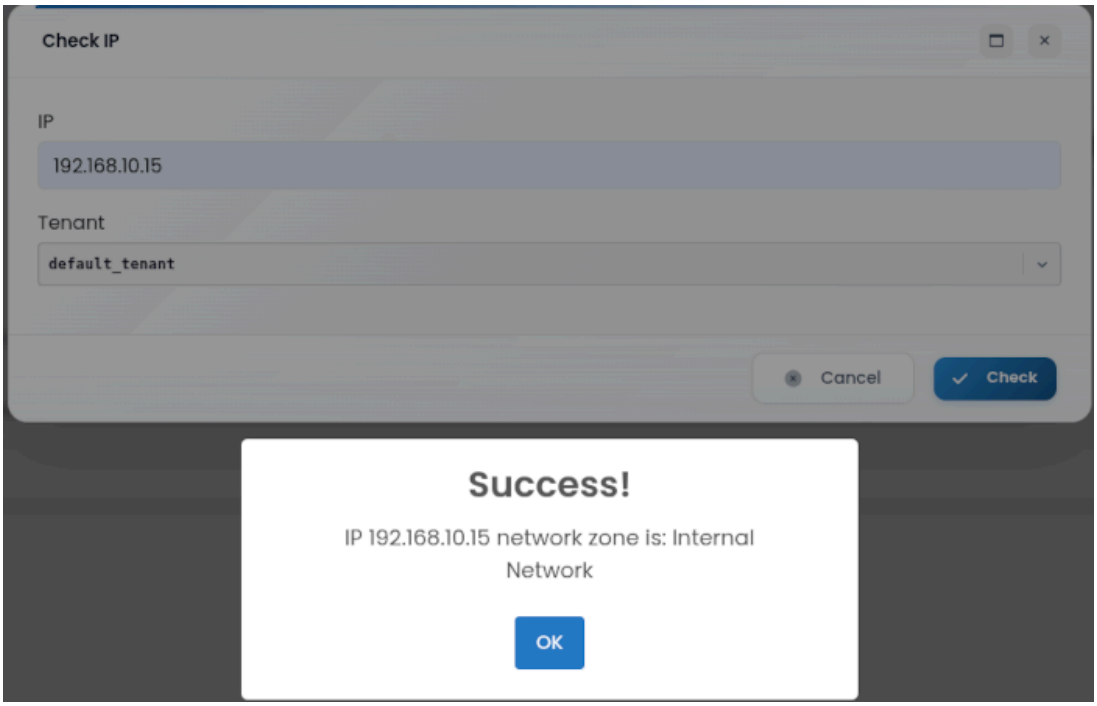


- **Edit Network** - update the network's configuration and settings. Changes take effect immediately.
- **Delete Network** - remove the network from the system. Confirmation is required to prevent accidental deletion.

Check IP allows administrators to verify whether a specific IP address belongs to a defined network segment by pressing the



button. This helps ensure accurate network mapping, proper monitoring, and correct assignment of security policies.



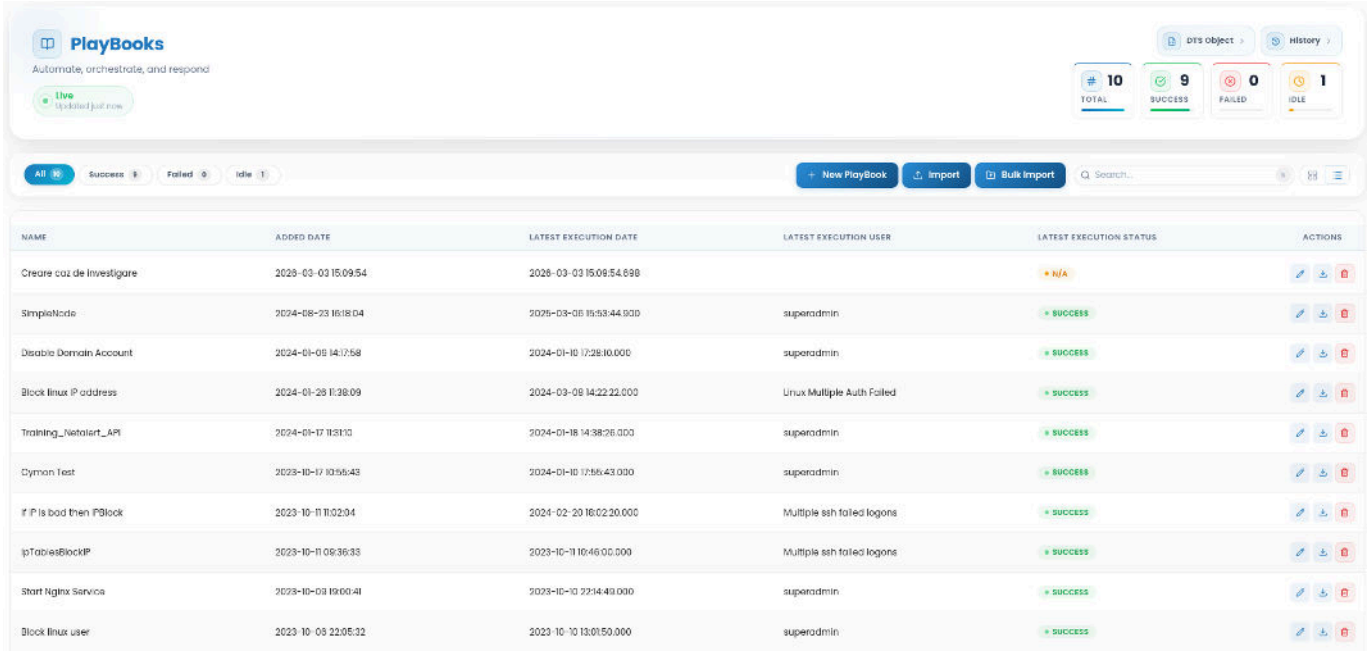
- **IP** - enter the IP address to verify which network segment it belongs to.
- **Tenant** - select the organizational unit or group to check the IP against its assigned network segments.

After entering the information, click **Check** to verify the IP or **Cancel** to exit without checking.

PlayBooks

Playbooks - automate and simplify the incident response process, helping security teams respond quickly and effectively to threats. They follow industry best practices, regulations, and organizational policies to ensure a consistent, coordinated approach that reduces the impact of security incidents and enables fast remediation.

To access the **Playbooks** interface, navigate to **Settings > Management > Playbooks**. The page will then open.



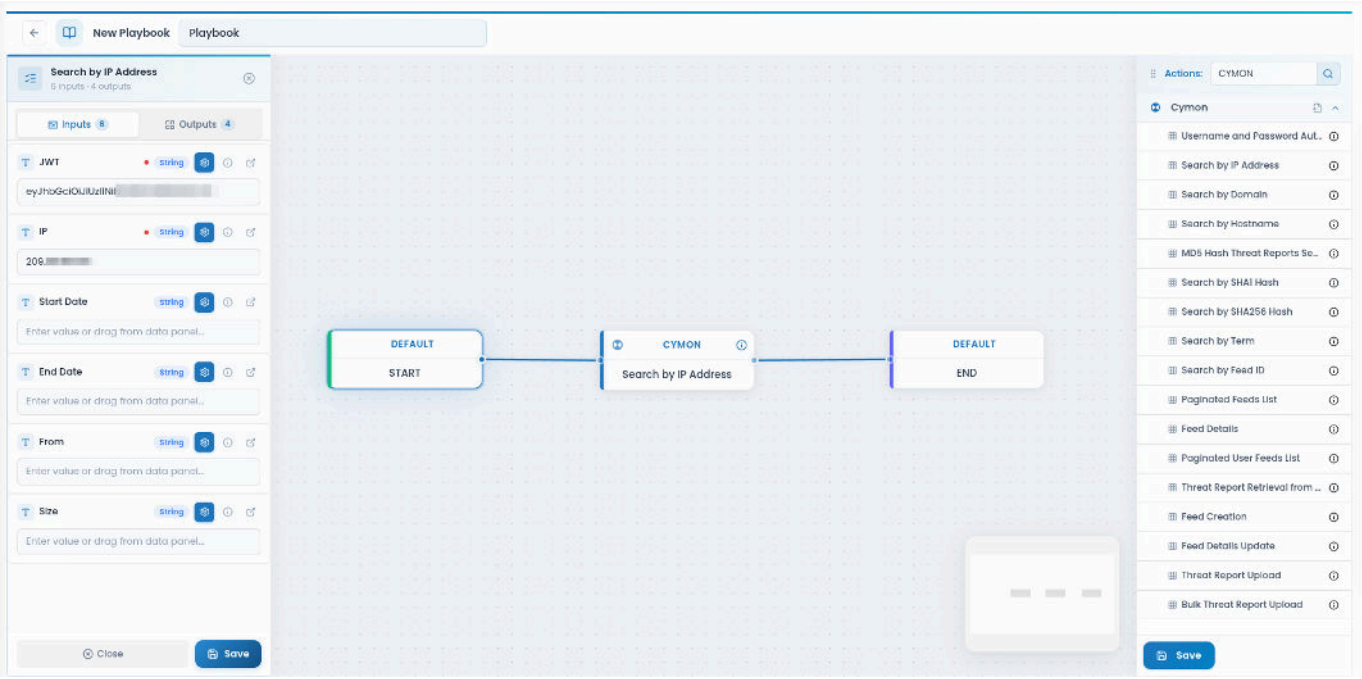
- **Event Trigger**: CYBERQUEST detects a suspicious event, like a network intrusion attempt or a high-severity alert from a security device. Playbook execution can be triggered automatically by an alert or manually from event or alert actions.

Playbooks can be added, edited, or deleted as needed.

Adding a Playbook

To add a new Playbook and orchestrate actions, click **New Playbook**. Playbooks are built visually, with two required blocks: **Start** and **End**.

Actions are executed according to the criteria set in the Playbook. Available actions are grouped by vendor and can be added using drag-and-drop.



Certain actions are triggered only when specific conditions are met.

Actions share information through an environment object, which stores alert or event data that can be used by subsequent actions.

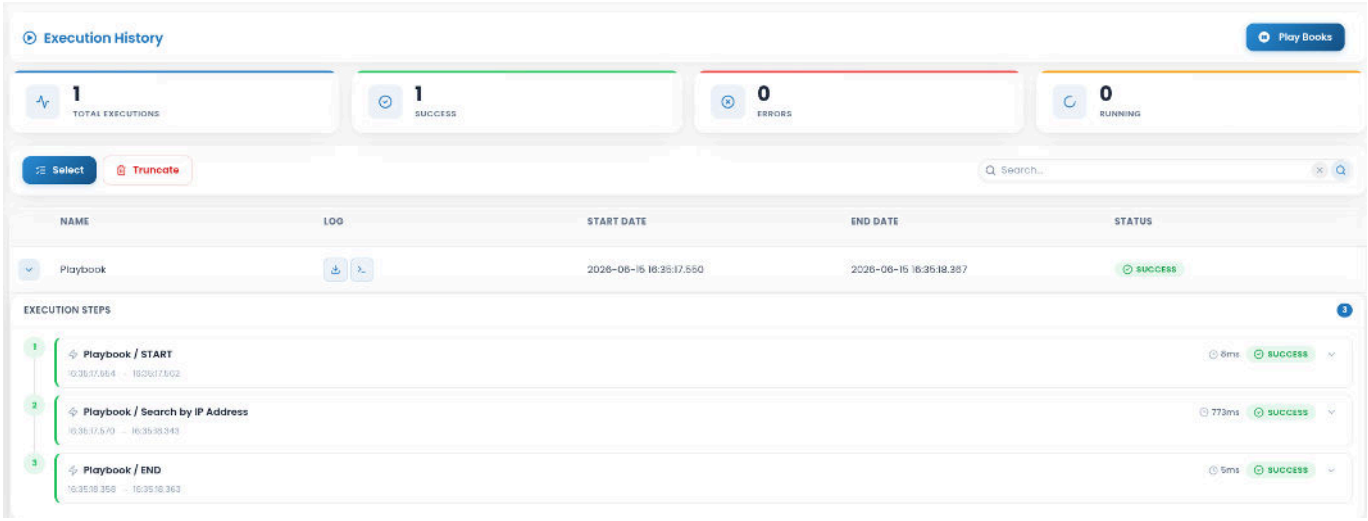
The environment object is defined as follows:

```
{
"Event":{
// ... the event which gets populated automatically by CyberQuest
},
"Alert":{
  // ... the alert which gets populated automatically by CyberQuest
}
"playbookGUID": // the individual playbook definition,
"startDate": 1685004728 // unix timestamp
"endDate": 1685004728  // timestamp
"status": "SUCCESS"
"history":[
    {
      "inputEnviroment":{
      // gets populated on the input enviroment of the individual step
      },
      "outputEnviroment":{
      // gets populated on the output enviroment of the individual step
      },
      "startDate": 1685004728 // unix timestamp
      "endDate": 1685004728  // timestamp
      "status": "SUCCESS"
    }
]
}
```

During execution, CYBERQUEST updates the environment object to record the execution history and log details. All actions have access to this object.

Execution History

Every action creates execution logs that help with debugging Playbooks and actions. If an error occurs, these logs can be reviewed to identify the cause, making troubleshooting easier and ensuring Playbooks run correctly and reliably.



Playbook logs can be **downloaded** in .txt format by clicking the



button, or **viewed** by clicking the



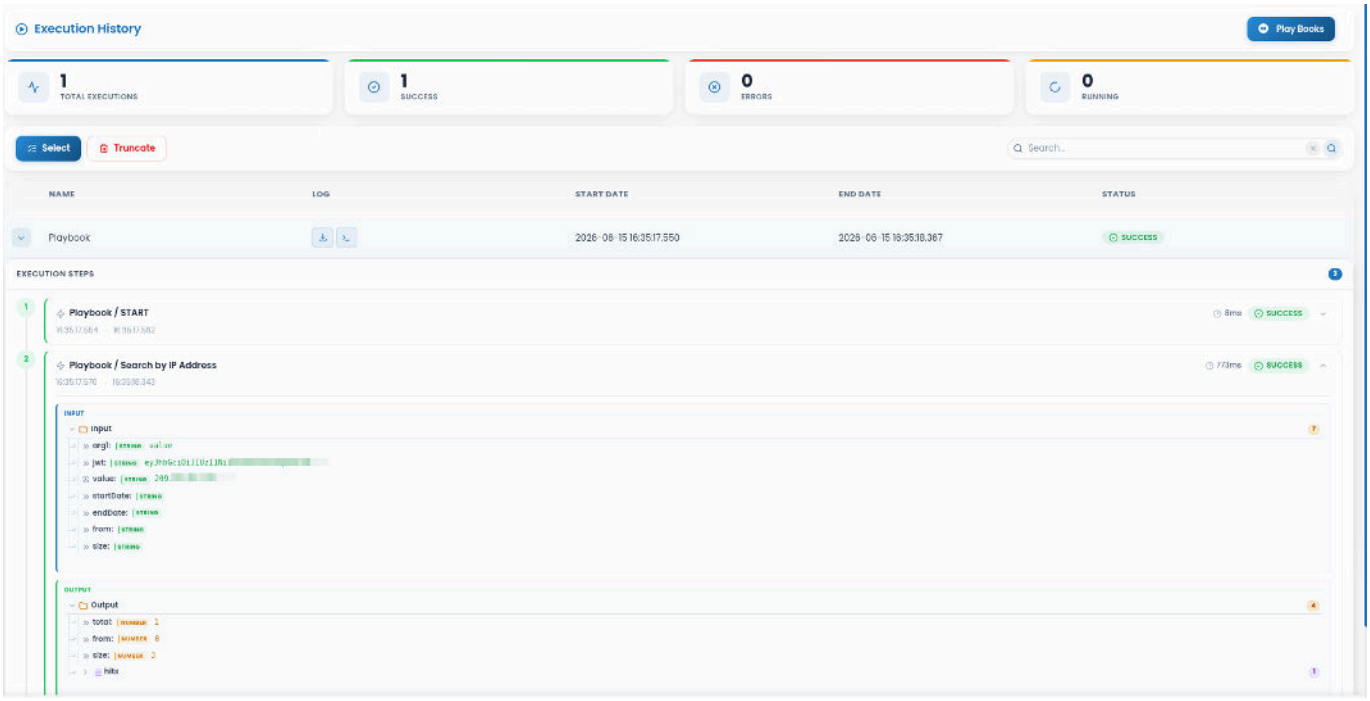
button.

Viewing Execution History

Click the



button in **Execution History** to view the input parameters and output data for each step of the execution.



Service Level Agreement (SLA) Management

Service Level Agreements (SLAs) in CYBERQUEST provide a structured framework for defining and enforcing response and resolution time commitments for security incidents and cases. SLAs ensure that security teams meet organizational performance standards, comply with regulatory requirements, and maintain consistent incident response timelines. By automating time tracking and escalation processes, SLAs help optimize resource allocation and improve overall security operations efficiency.

Navigate to **Settings > Management > Service Level Agreement (SLA)** in the Web Interface to access the SLA management page. This interface displays all configured SLAs and provides tools for creating, editing, and managing SLA definitions.



Name: Descriptive name for the SLA that clearly indicates its purpose and scope (e.g., “Critical Incident SLA”).

Description: Comprehensive explanation of the SLA’s purpose, applicable scenarios, and any special considerations.

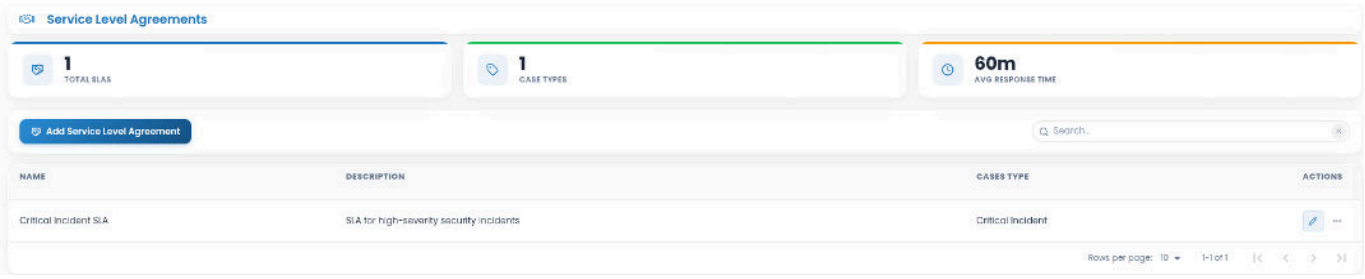
Case Types: Select one or more case types from the dropdown list that this SLA will apply to. These case types are predefined in Case Management and represent categories of incidents.

Confirmation Time (minutes): Maximum time allowed for acknowledging and assigning a case after creation. This represents the initial response commitment.

Response Time (minutes): Maximum time allowed for resolving a case after acknowledgment. This represents the resolution commitment.

Click “Save” to persist your configuration or “Cancel” to discard changes

Once an SLA is created, the following actions can be performed on it:



- **Editing SLAs** - Modify SLA parameters, case type associations, or time commitments using the **Edit**

  button. Changes take effect immediately for all active and future cases, while historical SLA compliance data remains unchanged.

- **Deleting SLAs** - Remove an SLA using the **Delete**

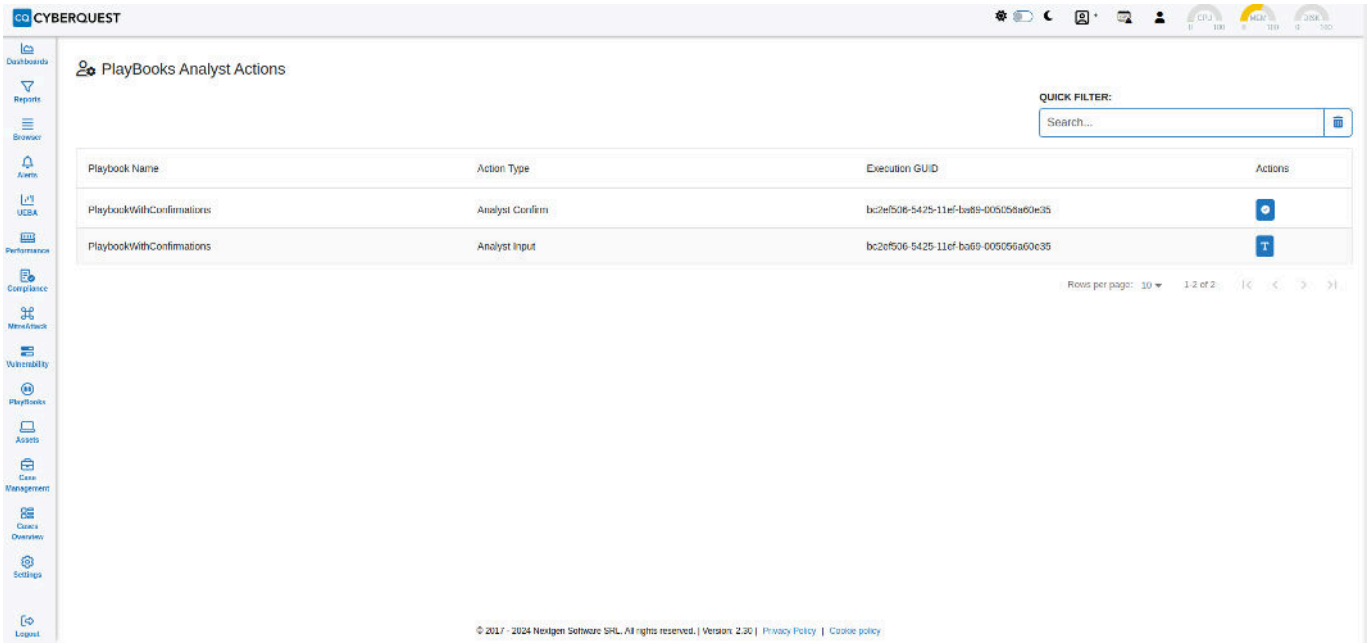
  button. Confirmation is required to prevent accidental deletion. Deleted SLAs no longer apply to future cases, but historical data is preserved.

Case confirmation and response times are automatically determined by the assigned SLA: Case Overview

Analyst Actions Management

Analyst Actions in CYBERQUEST provide a human-in-the-loop automation capability that allows playbooks to pause execution and request input or confirmation from security analysts during critical decision points. This feature enables automated workflows to incorporate human judgment, expertise, and situational awareness, ensuring that complex security decisions benefit from both automated efficiency and human oversight. Analyst Actions are essential for scenarios requiring ethical considerations, legal compliance, risk assessment, or complex judgment that cannot be fully automated.

Navigate to **Settings > Management > Analyst Actions** in the Web Interface to access the Analyst Actions management interface. This page displays all pending analyst questions and provides tools for managing and responding to them.



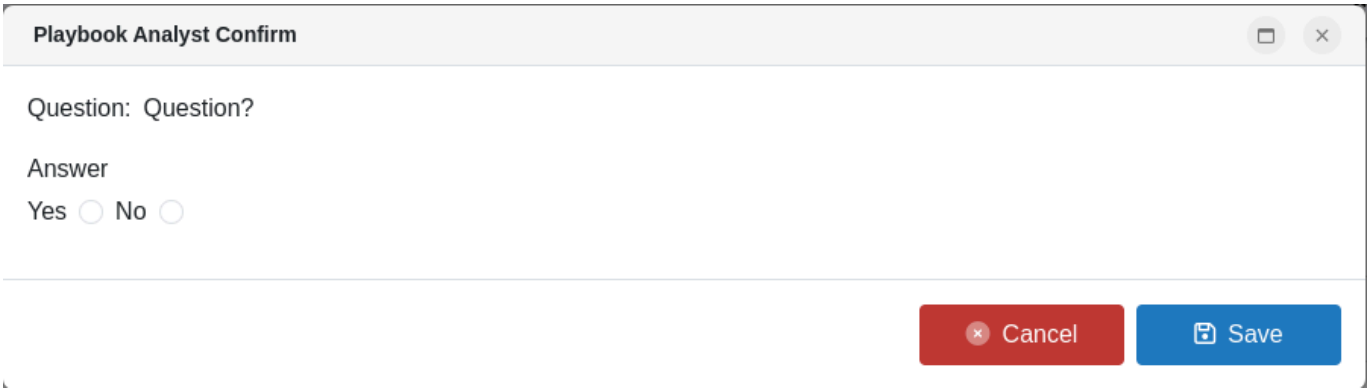
To continue execution, the analyst must respond when prompted. If no response is given within the timeout set in the action module, the default action defined at the action level will be applied automatically.

To respond to an Analyst Confirmation action:

1. Click the confirmation button



next to the action
2. The confirmation window will open with details of the request:

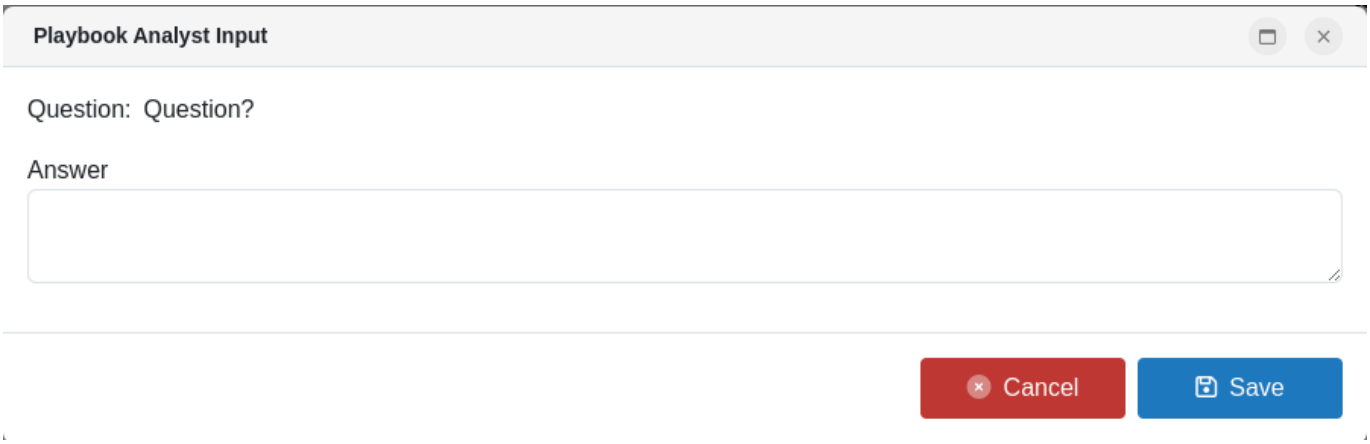


To respond to an Analyst Input action:

1. Click the input button



next to the action
2. The input form window will open with the request details:



Once the answer is saved, the action is removed and execution continues using the provided response.

Internal Security Documents

The **Internal Security Documents** module is the centralized repository for all files related to internal governance, security controls, operational procedures, and compliance evidence. It serves as the organization's **permanent archive**, ensuring long-term accessibility and traceability of all uploaded materials.

Navigate to **Settings > Management > Internal security documents** in the Web Interface to access the Internal security documents management interface.



This module allows users to:

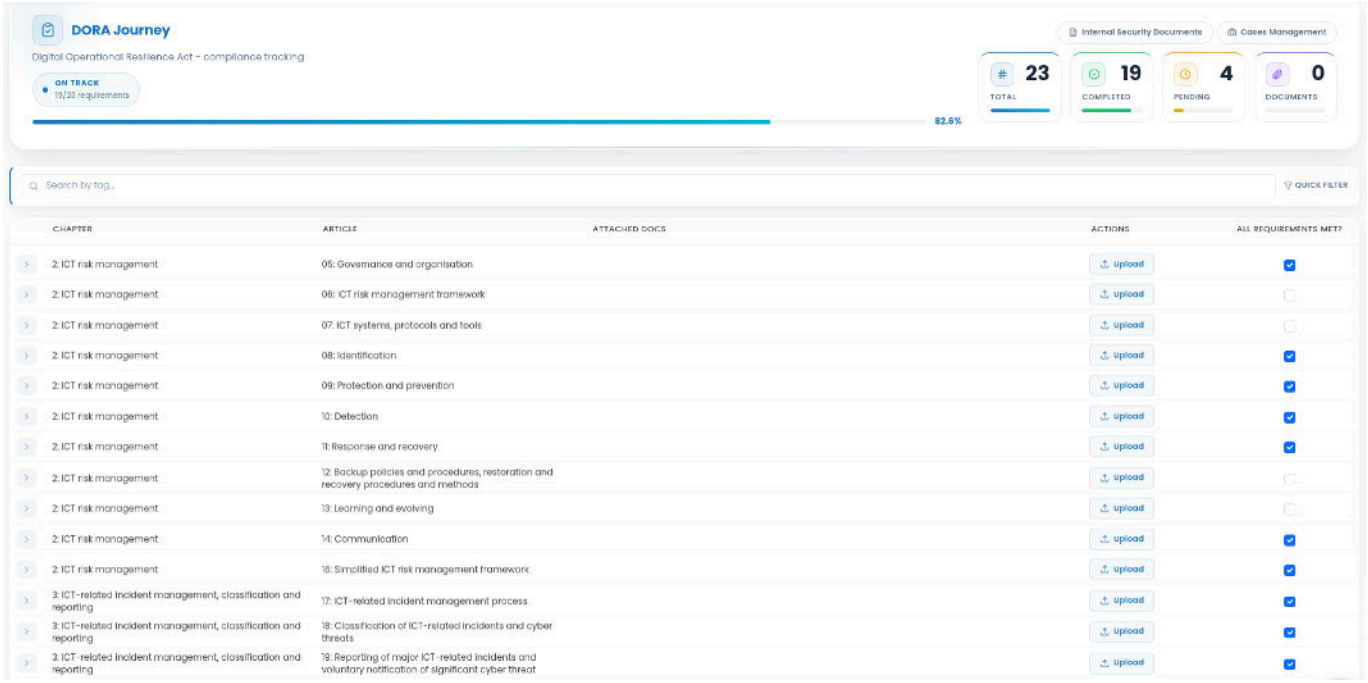
- Upload internal security or compliance-related documents
- View all historical and current documents in a single, consolidated archive
- Download/export files for audits, internal reviews, or regulatory requests
- Delete outdated or irrelevant documents (this action affects only this repository)
- Maintain an independent record of every version and upload event over time

The repository uses a **non-destructive retention model**:

- Each upload appears as a separate entry
- Updated versions do not overwrite older ones
- A complete chronological history is preserved unless files are manually deleted

DORA Journey

The **DORA Journey** module guides organizations through the Digital Operational Resilience Act (DORA) compliance process. Each requirement, article, or chapter may require supporting documentation (evidence).



When completing a DORA requirement:

- Users **must upload documents directly from within the DORA Journey interface**
- These files are attached as evidence exclusively to the selected requirement
- **All requirements met?**

  Marks the section as complete once all mandatory evidence and actions have been provided.

Important: *Documents already stored in Internal Security Documents* ***cannot be selected or reused*** *inside DORA Journey.* New uploads are always required for each piece of evidence.

What Happens to Documents Uploaded in DORA Journey

Any document uploaded in DORA Journey is:

- Stored as evidence in the specific DORA requirement
- **Automatically added** as a separate entry in the Internal Security Documents repository

If a document is later removed or replaced inside DORA Journey:

- The removal only applies to DORA Journey
- The original and previous versions remain preserved in Internal Security Documents

Interaction Between Internal security documents and DORA Journey

Although they operate separately, the modules interact in a structured way:

- Upload from **Internal Security Documents - NOT available in DORA Journey**
- Upload from **DORA Journey - automatically stored in Internal Security Documents**

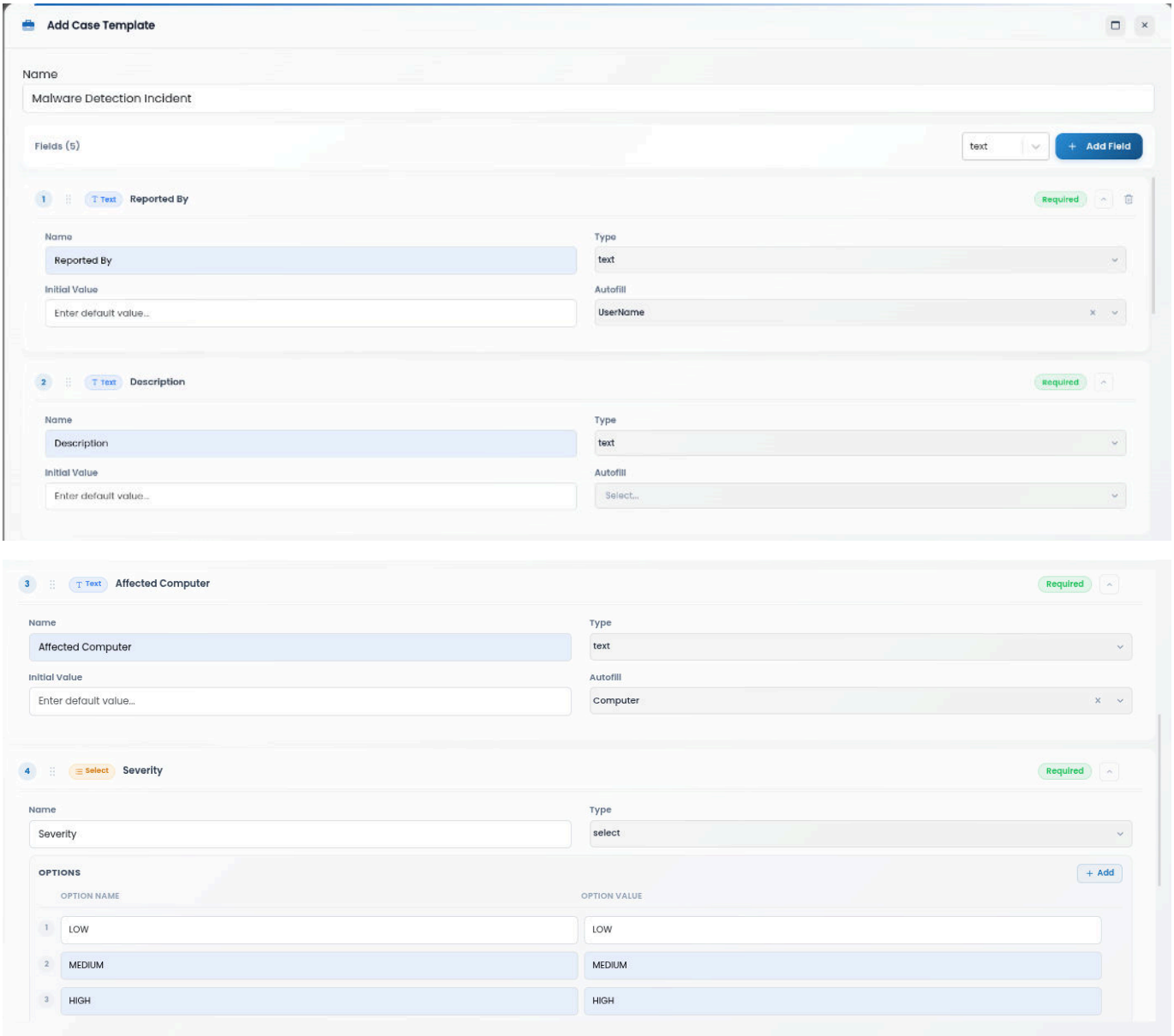
The **Internal Security Documents** module functions as a permanent archive, preserving every version of every uploaded file. The **DORA Journey** module, by contrast, is dedicated solely to submitting evidence for DORA requirements and always requires new uploads any deletions or updates made within DORA Journey have no impact on the documents stored in Internal Security Documents.

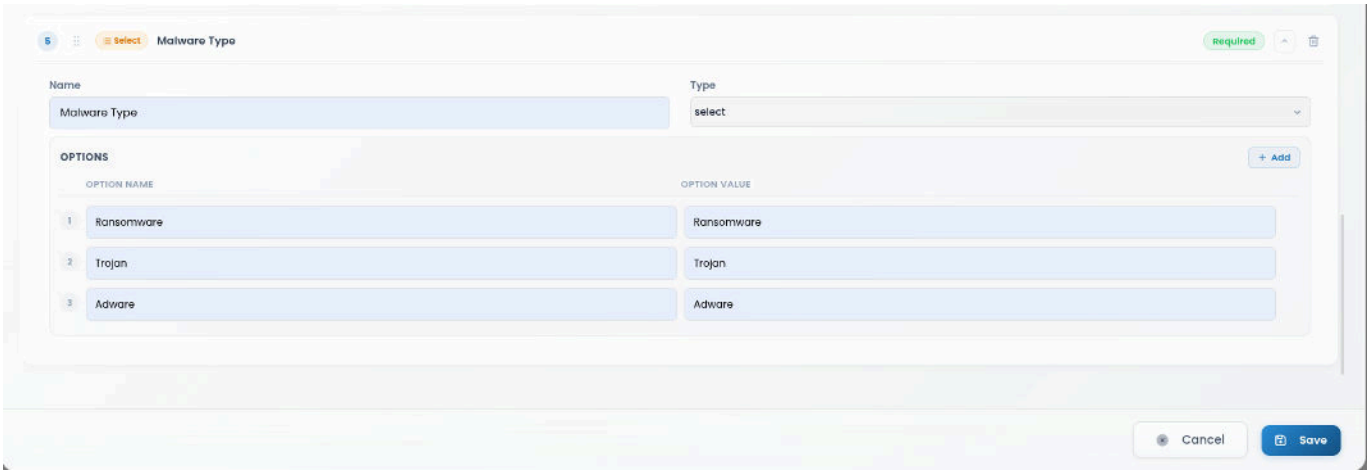
Case Templates

Case Templates in CYBERQUEST allow administrators to define reusable field structures for case creation, ensuring consistency and efficiency across all cases. Each template contains predefined fields that can capture information in four formats: **text**, **boolean** (true/false), **select** (dropdown options), and **float** (numeric values with decimals).

Templates can include:

- **Text fields** for entering free-form information like usernames or descriptions.
- **Select fields** for choosing from predefined options.
- **Boolean fields** for simple yes/no or true/false inputs.
- **Float fields** for numeric values with decimals.

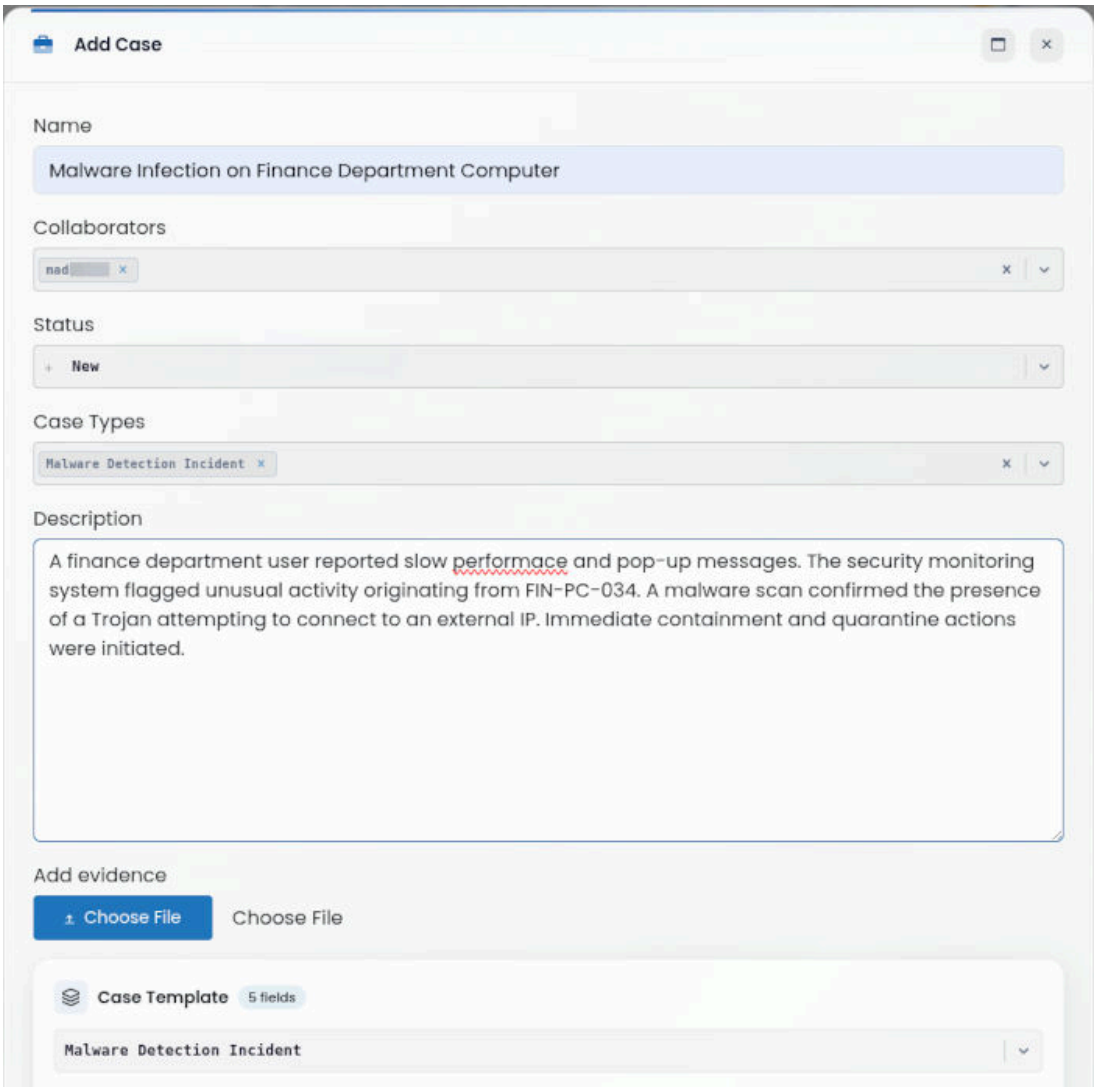


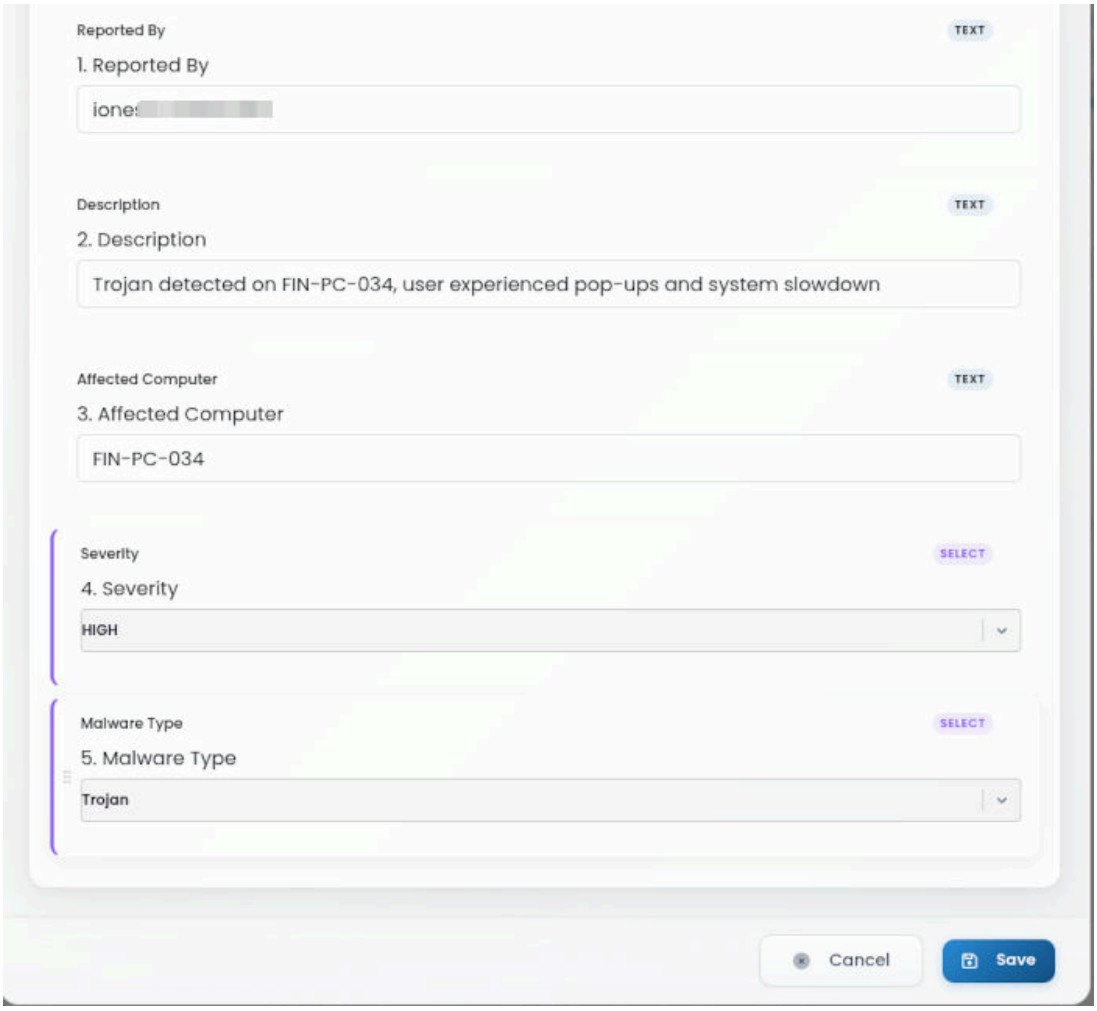


Once a **Case Template** is created, it can be used to generate new cases in the **Case Management** module. This ensures that every case follows the same predefined structure and captures all required details for analysis, reporting, and tracking.

Creating a New Case Using a Case Template

To create a new case using a case template, navigate to ***Case Management > New Case***, select the desired template from the **Template** drop-down list, fill in the required case details, and save.



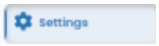


Jobs

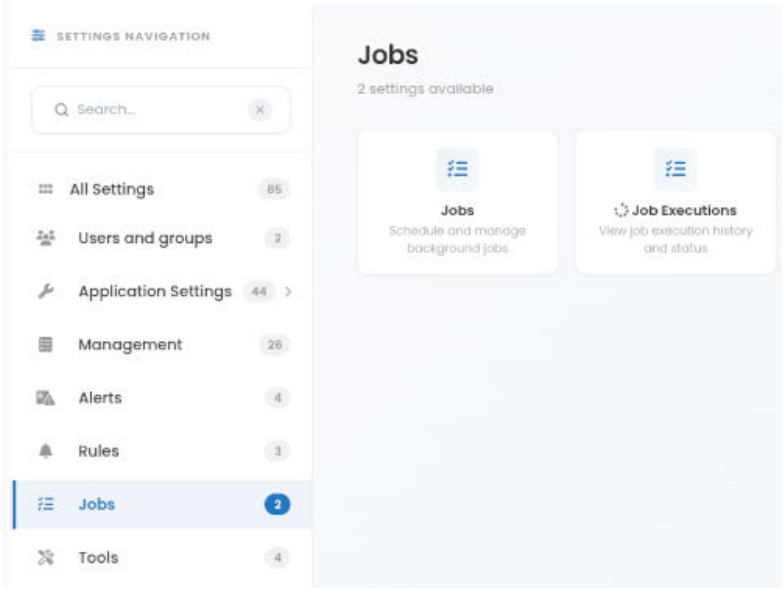
Jobs can be created and used to process data stored in the online or archive repositories. Since these repositories can grow significantly over time, and due to restrictions on manipulating data while in use or at different stages of its lifecycle, directly copying, moving, or deleting storage files is not recommended.

To access the **Jobs** functionality:

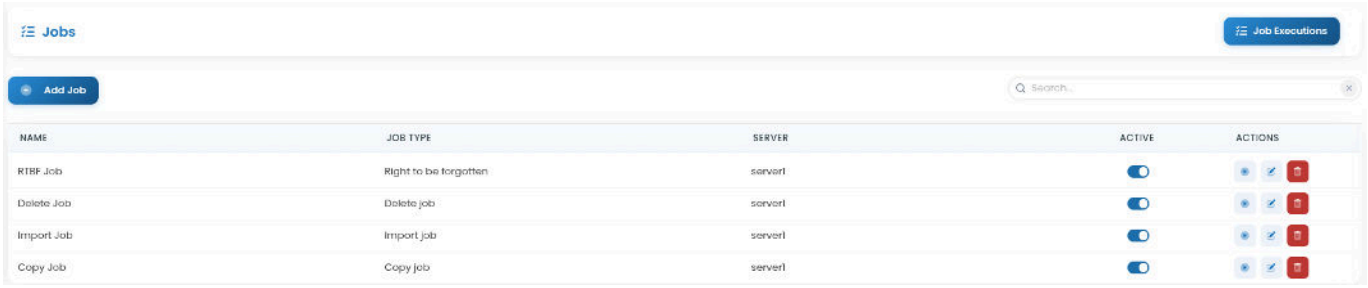
1. Navigate to **Settings** by pressing the settings button

   in the top-right corner of the interface
2. Click **Jobs** > **Jobs** from the navigation menu



The **Jobs** page opens, displaying the list of existing jobs and providing the option to create a new one. Initially, no pre-defined jobs are available.



- **Execute a job**: Click the start job

  button to run a job. Job executions can be monitored in the Job Executions section.

- **Delete a job**: Click the delete

  button next to a job. A confirmation dialog will appear to prevent accidental deletions.

- **Activate/Deactivate a job**: Click the status

  button to enable or disable a job. Inactive jobs will not execute automatically.

  An unlimited number of jobs can be created, with the primary consideration being the load their execution may impose on the solution environment. Jobs can be resource-intensive, potentially impacting the server's processor, memory, storage, and network.

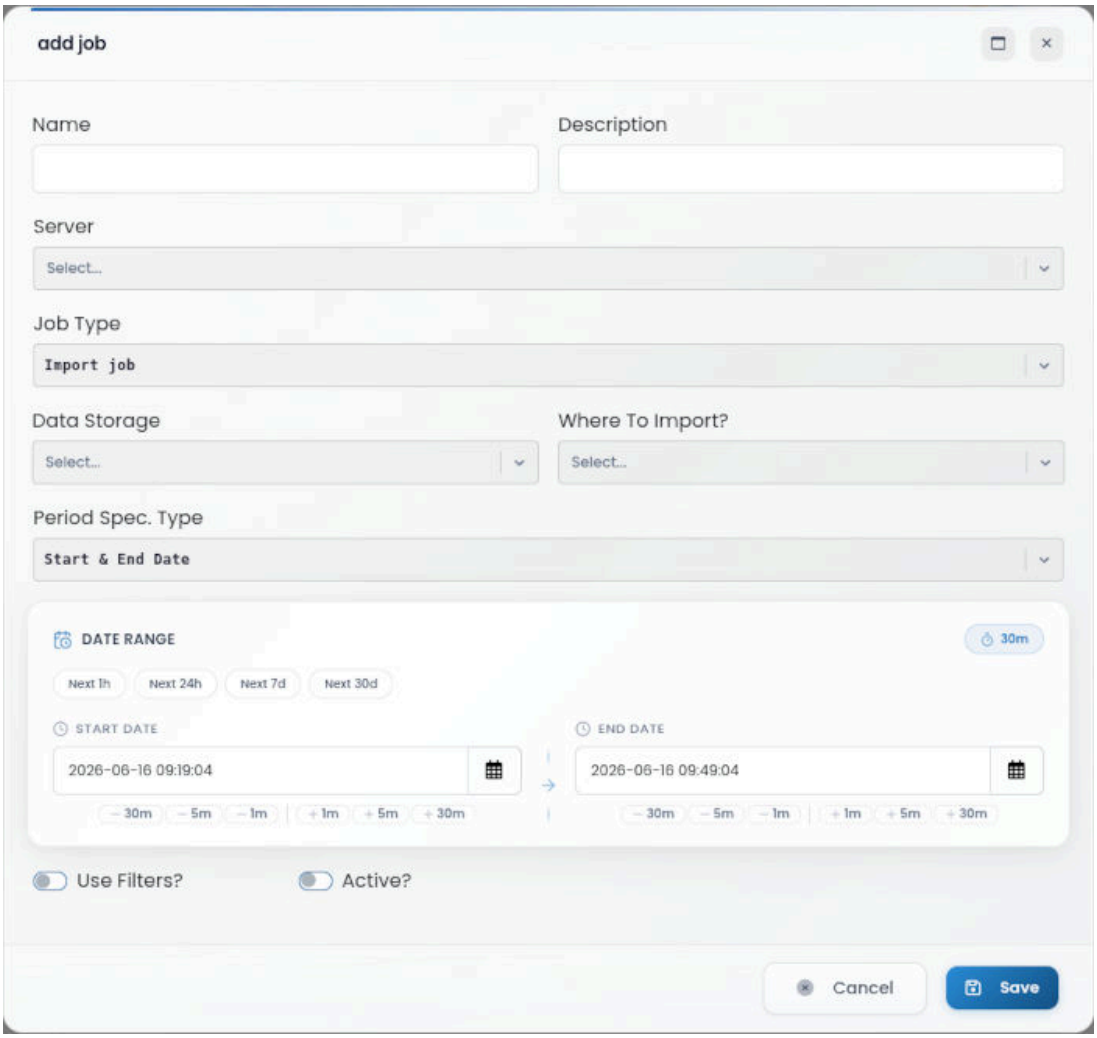
  The list of existing jobs provides details on the job type, the server on which it is executed, and its active status. Further explanations of these details are provided in the section on creating a new job.

Creating a New Job

To create a new job navigate to **Settings** > **Jobs** > **Jobs**, click the add job



button and the Job Configuration page will open



The following attributes are available in both Create and Edit Job configuration pages. Note that available options may vary based on the selected job type.

- **Name**: Enter a descriptive name that uniquely identifies the job. This name will appear in the Jobs list and execution logs.
- **Description**: Provide a detailed explanation of the job's purpose and what it accomplishes. This helps with documentation and troubleshooting.
- **Server**: Use the dropdown to select the target data server where the job will execute. Choose a server with adequate resources for the job's requirements.
- **Job Type**: Select the type of operation to perform:
  - **Import Job**: Transfers events from a source repository to an online or archive repository. Import jobs are very useful for consolidation operations, or when decommissioning obsolete repositories.
  - **Delete Job**: Removes events from a repository to free up storage space. Common use cases include cleaning up data from obsolete applications, removing data following successful import operations, and performing compliance-driven data purges. Deletions are permanent, so proper backups and testing should be ensured before execution.
  - **Copy Job**: Duplicates data from one storage location to another, creating exact copies of the source data. Common use cases include creating offline backups, performing data analysis on copied datasets, and setting up testing environments with production-like data.
  - **Right to be Forgotten (RTBF)**: Performs granular deletion of personal data based on specific criteria, supporting compliance with privacy regulations and fulfillment of data subject requests.

- **Data Storage**: Always specifies the source data storage, regardless of job type. This is where the data will be read from during job execution.
- **Where to Import**: Choose the destination for imported data:
  - **Online repository**: Data is extracted from the online repository and is governed by the repository's retention period (*Settings > Application Settings > Retention Period > RetentionPeriodEL*). This also applies to archived data within the retention period of the online repository, for instance, when the online repository needs to be recovered after an issue.
  - **Archive repository**:Data is extracted from the online repository with a special tag and is subject to the **RetentionPeriodArchive** parameter (Settings > Application Settings > Retention Period > RetentionPeriodArchive). This applies to data older than the retention period set for the online repository, such as when data from six months ago is needed for investigation while the online repository's retention period is only one month.
    - **Configuration**:
    - Check `RetentionPeriodArchive` parameter (in days) in Settings > Application Settings > Retention Period
    - Ensure the parameter covers the time period of events to be extracted

To remove archived data, reduce the `RetentionPeriodArchive` value - data older than the new period will be automatically deleted

- **Period Spec. Type**: Define the time range for job operations:
  - **Start & End Date**: Defines the exact date and time range for data processing. This is used when working with data from a specific period. Dates and times can be selected from a calendar or entered manually.
  - **Last 'x' Units**: Allows processing of the most recent data based on selected time units - seconds, minutes, hours, days, months, or years. This is useful for regularly handling recent data, for example, processing the last 7 days for weekly reports or the last 30 days for monthly data.
- **Active?**: Enable or disable the job. Inactive jobs will not execute automatically but can still be run manually.

After configuring all attributes, click **Save** to create the job and add it to the Jobs list, or click **Cancel** to close the window without saving any changes.

For practical guidance on implementing specific job types, refer to these detailed examples:

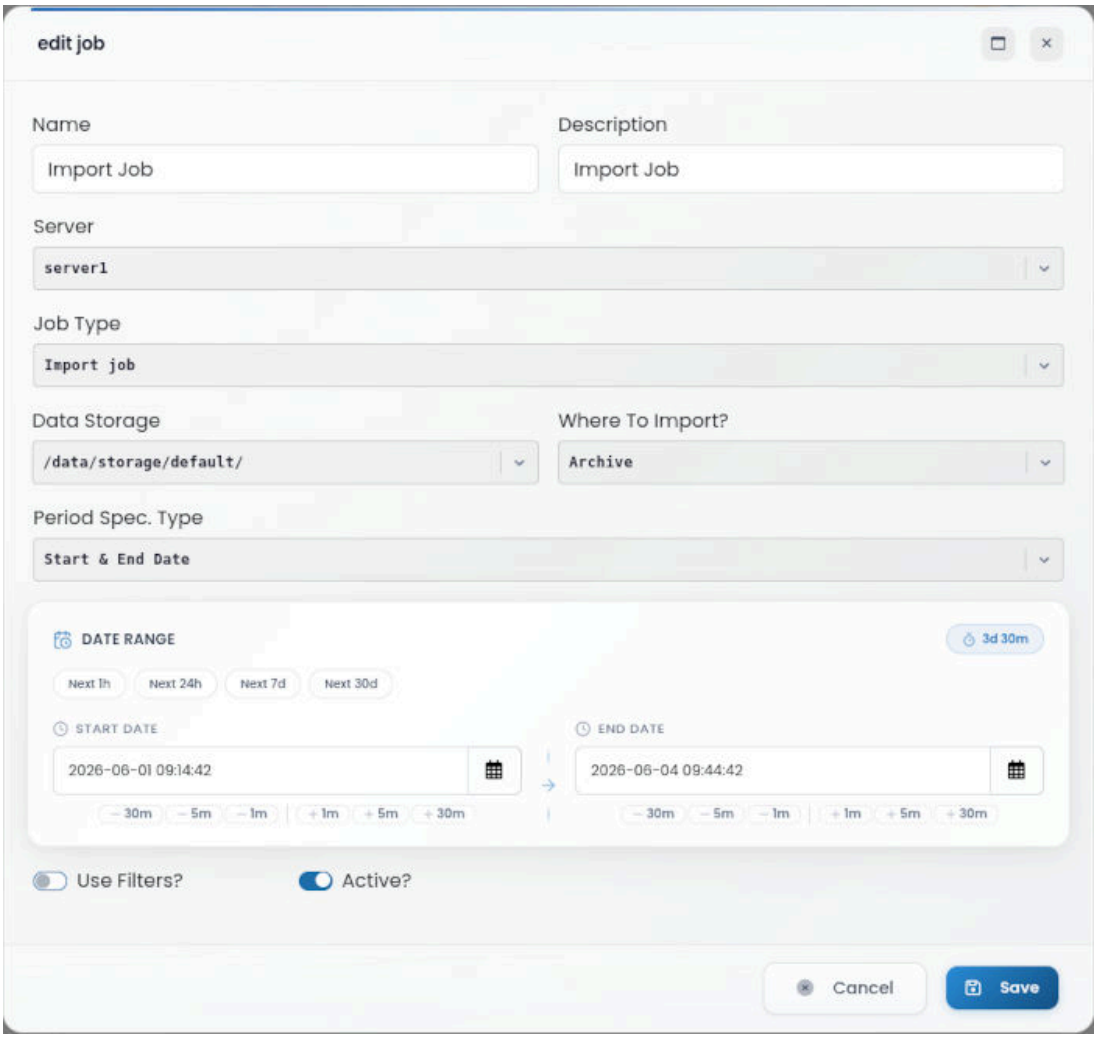
- How to restore data from archive
- How to create a Copy job
- How to create a RTBF job
- How to delete data from Data Storage

Manage Jobs

To modify an existing job, locate it in the Jobs list, click the edit

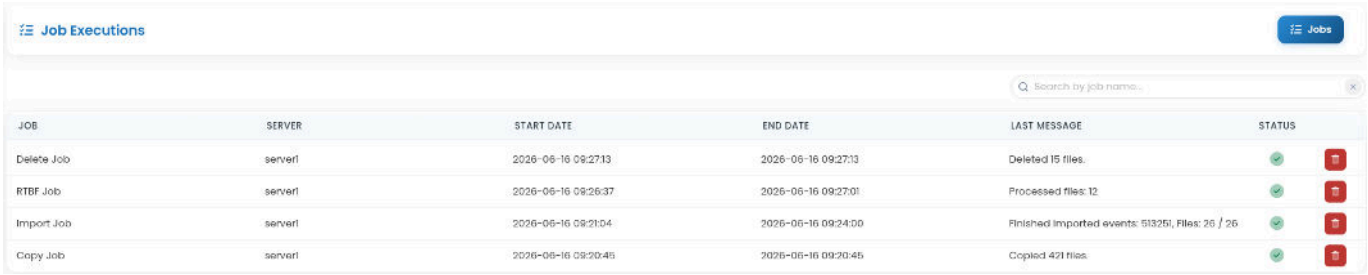


button, make the necessary changes on the **Edit Job** page, and then click **Save** to apply the updates and close the page.



Managing Job Executions

Go to **Settings > Jobs > Job Executions**. The **Job Executions** page opens, displaying the history of executed jobs, their results, and a summary of jobs currently in progress.



Deleting an execution from this list only has an effect if the job is still in progress. As a best practice, it is recommended to wait until an execution is complete before deleting it.

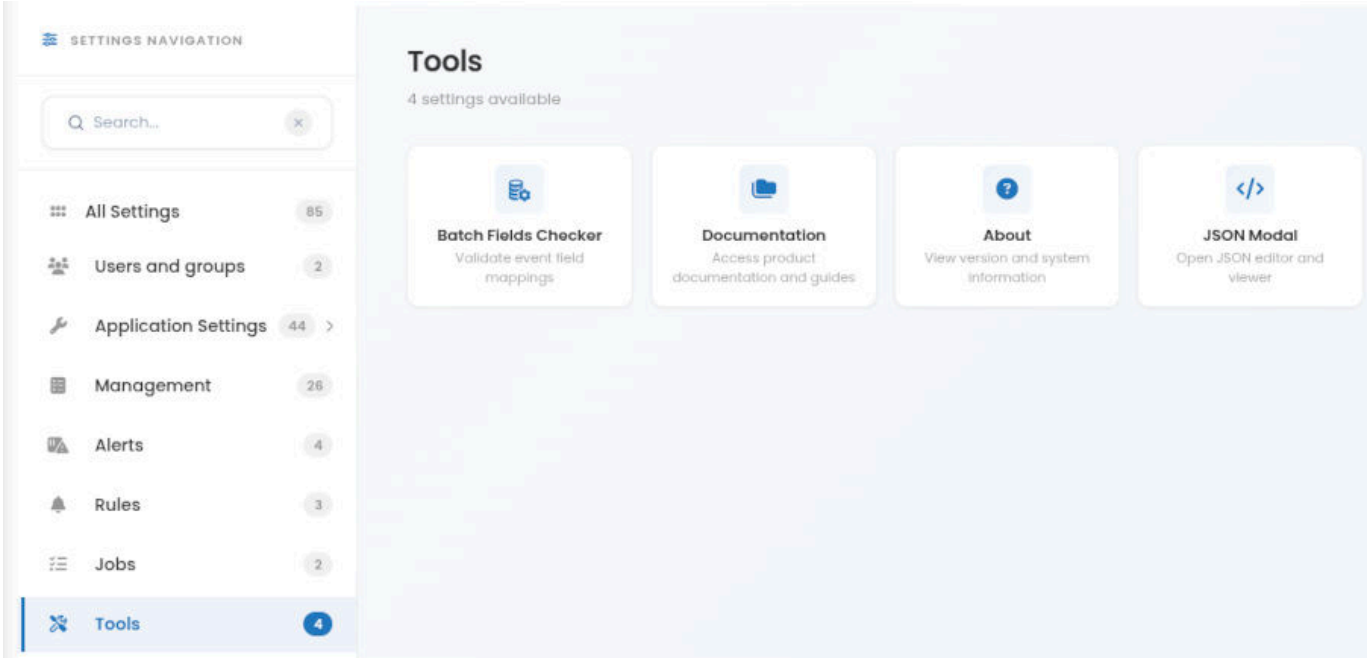
Tools

This section provides an overview of the available tools in CYBERQUEST that help with data processing, analysis, and system management.

Batch Fields Checker

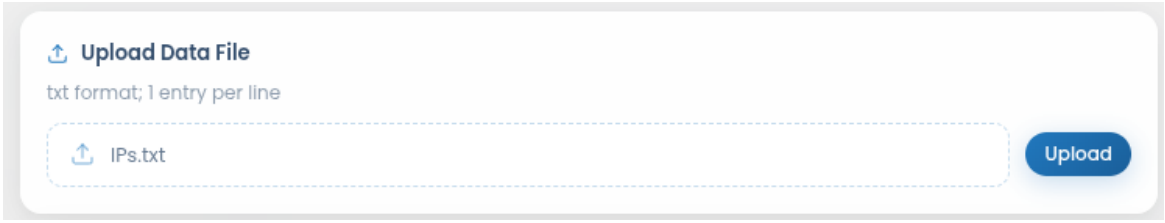
The **Batch Fields Checker** is a powerful tool designed for bulk data analysis and validation. It enables processing of large data volumes across multiple fields simultaneously, making it ideal for security analysts and system administrators who need to quickly identify patterns, validate data, or perform comprehensive searches across the CYBERQUEST platform.

Navigate to **Settings > Tools > Batch Fields Checker** from the CYBERQUEST Web Interface:



1.Create a text file containing the values to search for. Each value should be on a separate line.

2.Click **Choose File** to select the text file, then press **UPLOAD** to begin the process.



3.After uploading, select the specific fields to search across. The system will compare each value from the file with all selected fields. Common fields include:



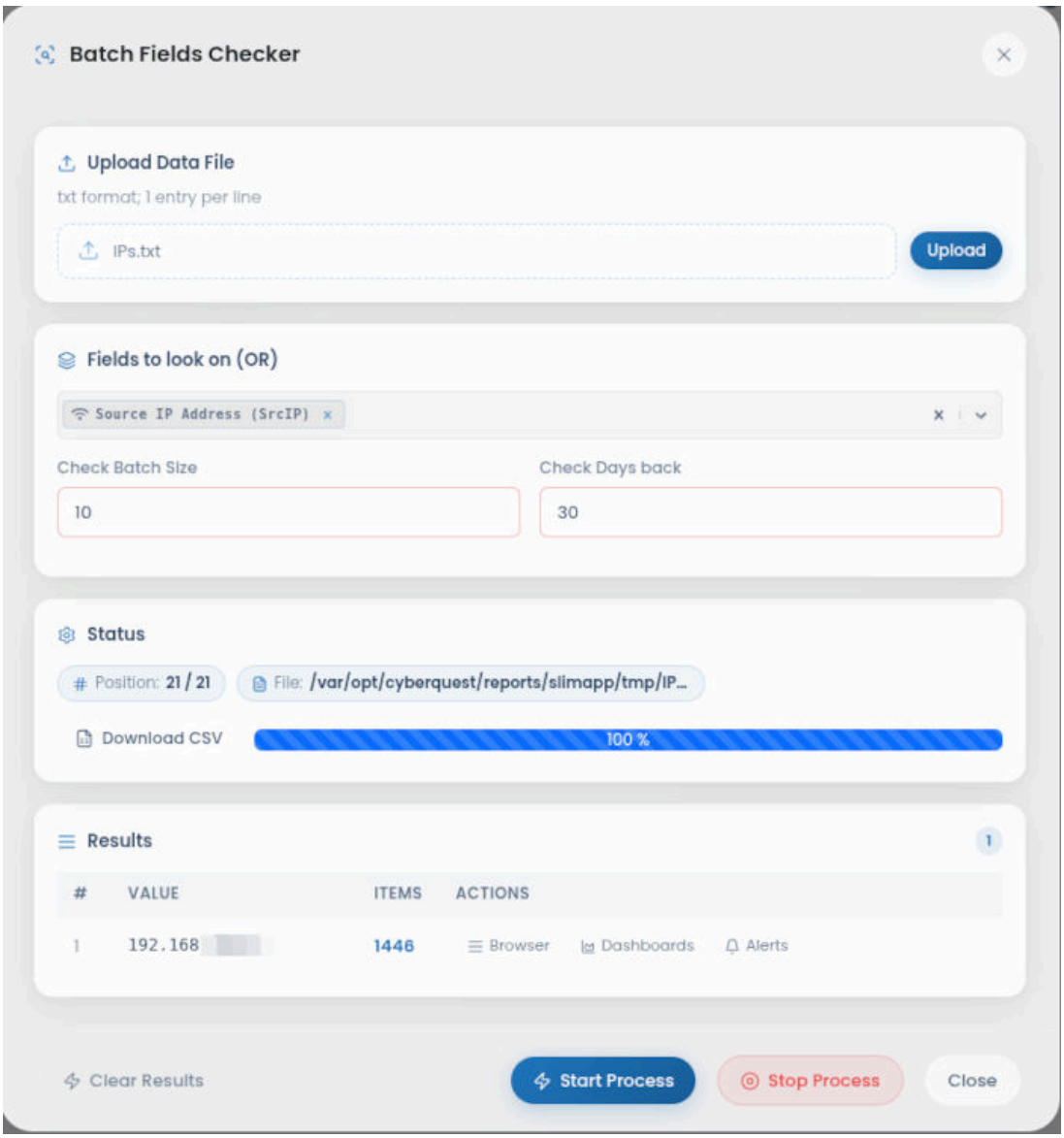
4.Configure search parameters:

- **Check Batch Size**: Specify how many lines from the file to process in this batch.
- **Check Days back**: Set the time range for the search (e.g., 7 days, 30 days, 90 days).

5.Click the start button



to begin processing.

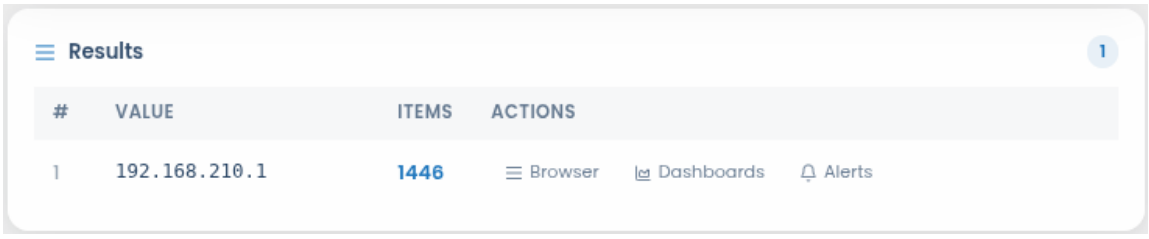


Current Position: Number of lines processed from the input file.

Current File: Location where temporary results are stored on the server

DOWNLOAD CSV: Export current results for immediate analysis

After processing completes, results are displayed with three key columns:



- **Value**: The original value from the input file.
- **Items**: Number of matches found for that value.
- **Actions**: Available actions for each result.

Results can be sent to:

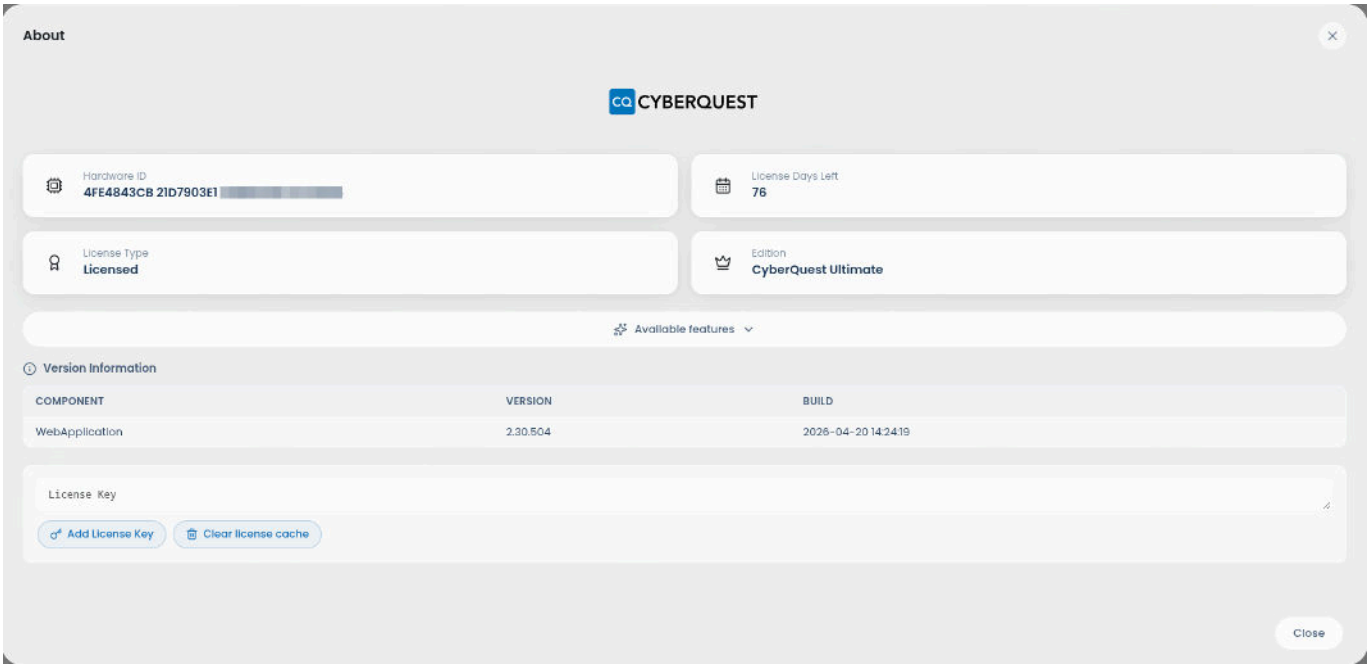
- **Browser**: For detailed investigation in the CYBERQUEST browser interface
- **Dashboards**: To create visual dashboards based on findings
- **Alerts**: To set up monitoring for specific patterns or values

Note: When using results in other modules, search within the same time range specified in **Check Days Back** to see consistent results.

About / Licensing

The **About** section provides comprehensive information about your CYBERQUEST instance and license management capabilities.

Navigate to **Settings > Tools > About** to open the **About CYBERQUEST** window:



The **About CYBERQUEST** window provides the following information:

- **Hardware ID**: Unique identifier for the CYBERQUEST machine. This ID is used for permanent license registration
- **License days left**: Remaining days of license validity.
- **License type**: Current license status:
  - **Licensed**: Full access to all features
  - **Not Licensed**: Limited functionality available
- **Edition**: The specific CYBERQUEST edition for which the license is registered.

To add a new license, copy the license key, paste it into the **License Key** field, and click **Add License Key**.

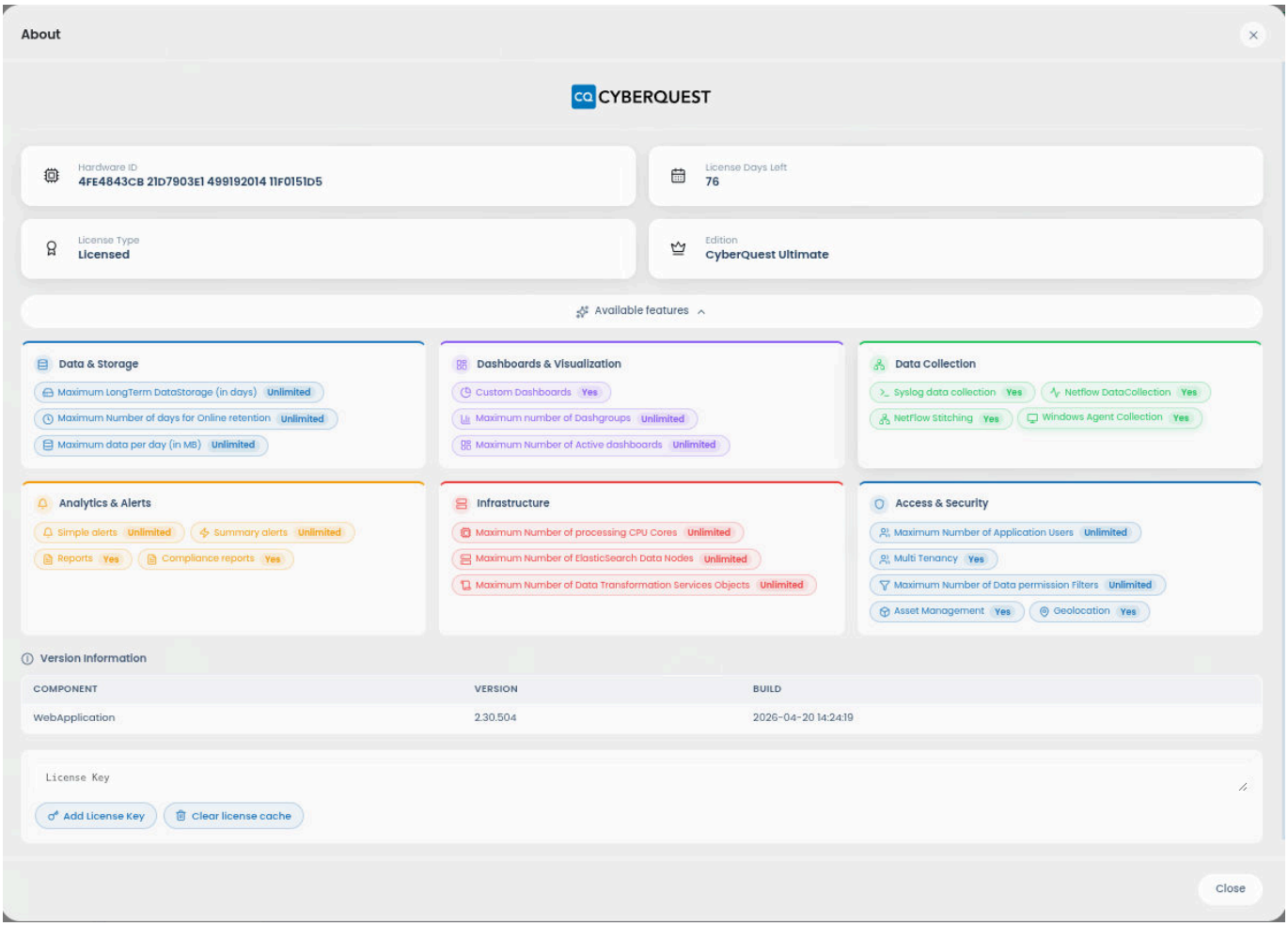
Important: New licenses can either replace the current license entirely or add additional functionality through add-on licenses.

The **Clear license cache** button forces the update of the license details in the web interface.

Expand the detailed information button



to view comprehensive license details including:



Marketplace Importing and Exporting Extensions

Marketplace: Importing and Exporting Extensions

Overview

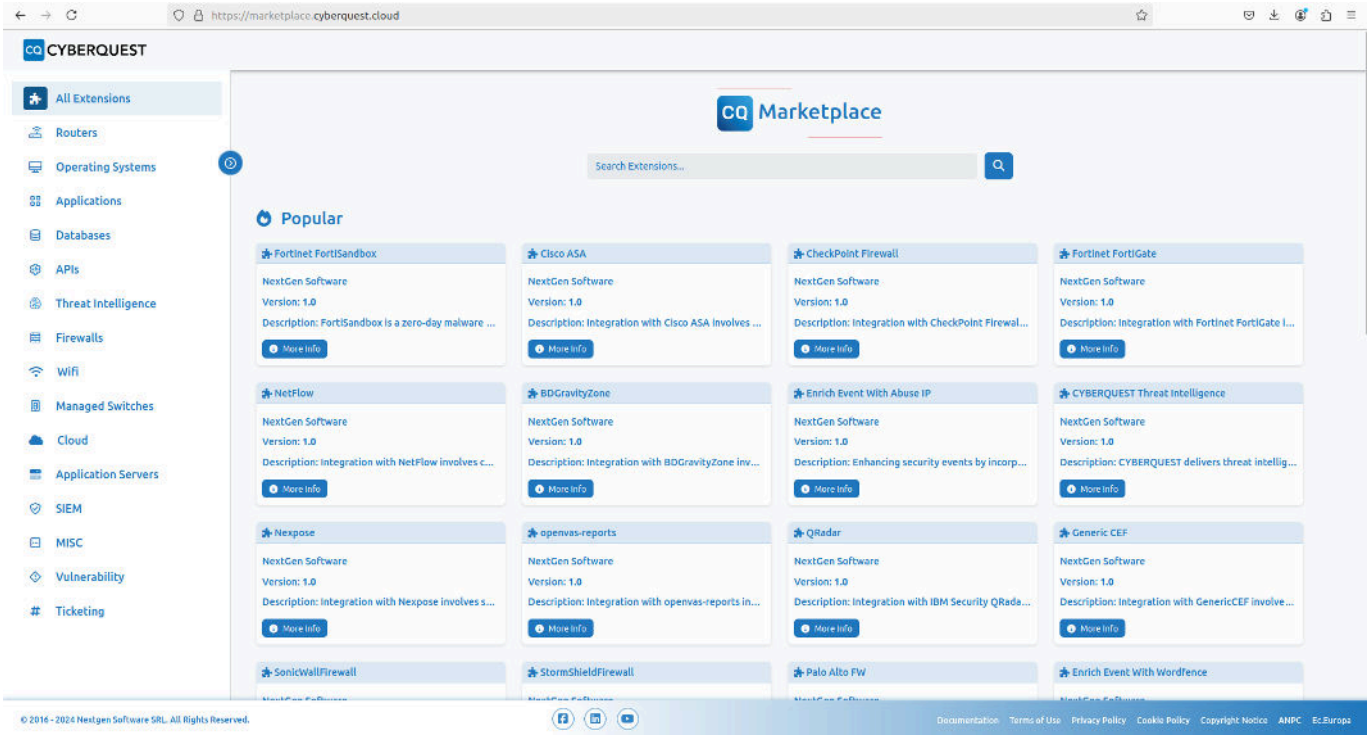
The CYBERQUEST Marketplace serves as a centralized repository for pre-built extensions, dashboards, and security components that enhance your CYBERQUEST security monitoring capabilities.

How to export extensions from Marketplace cloud

Exporting extensions from the Marketplace cloud allows downloading and saving extension files for later import into a CYBERQUEST instance.

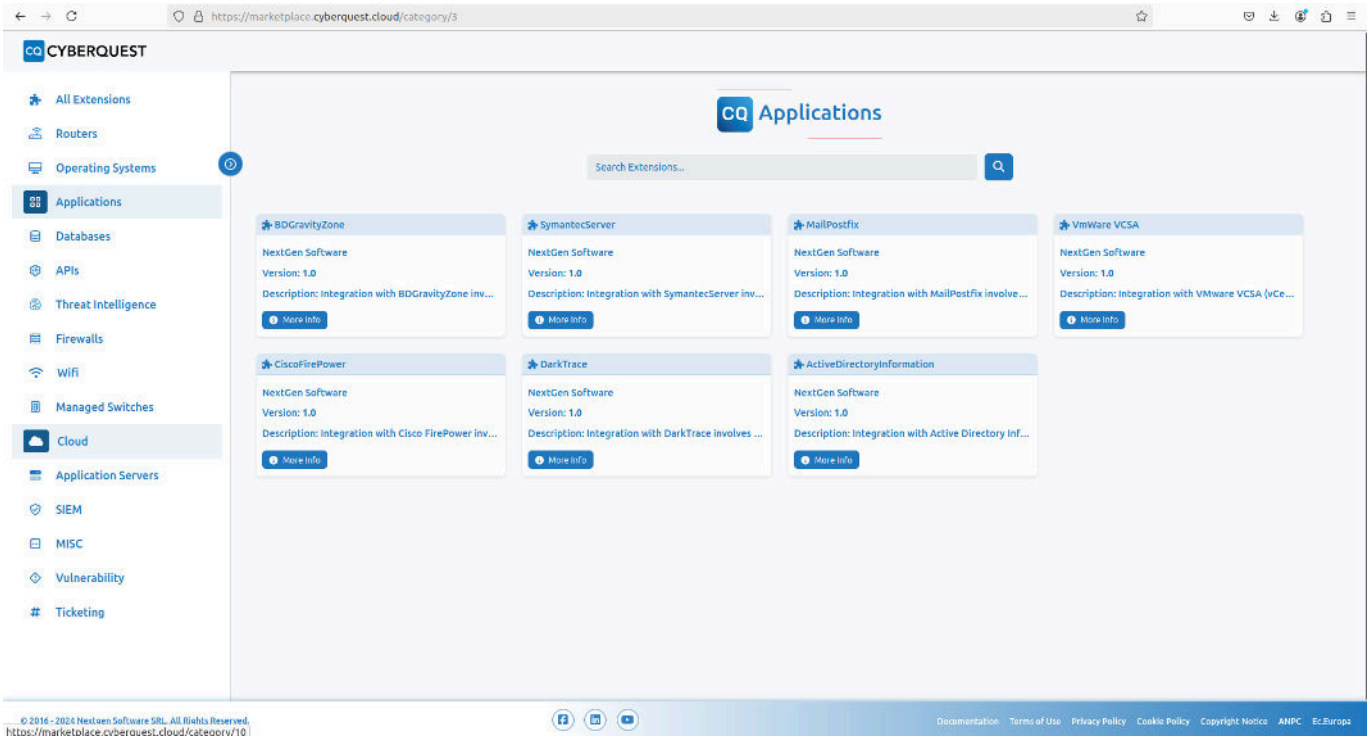
1.**Access the Marketplace Cloud**

Navigate to the official CYBERQUEST Marketplace at https://marketplace.cyberquest.cloud/ (https://marketplace.cyberquest.cloud/) using a web browser.



2.**Navigate to Extensions Section**

From the left-side menu in the web interface, select the **Extensions** option to view all available extensions.

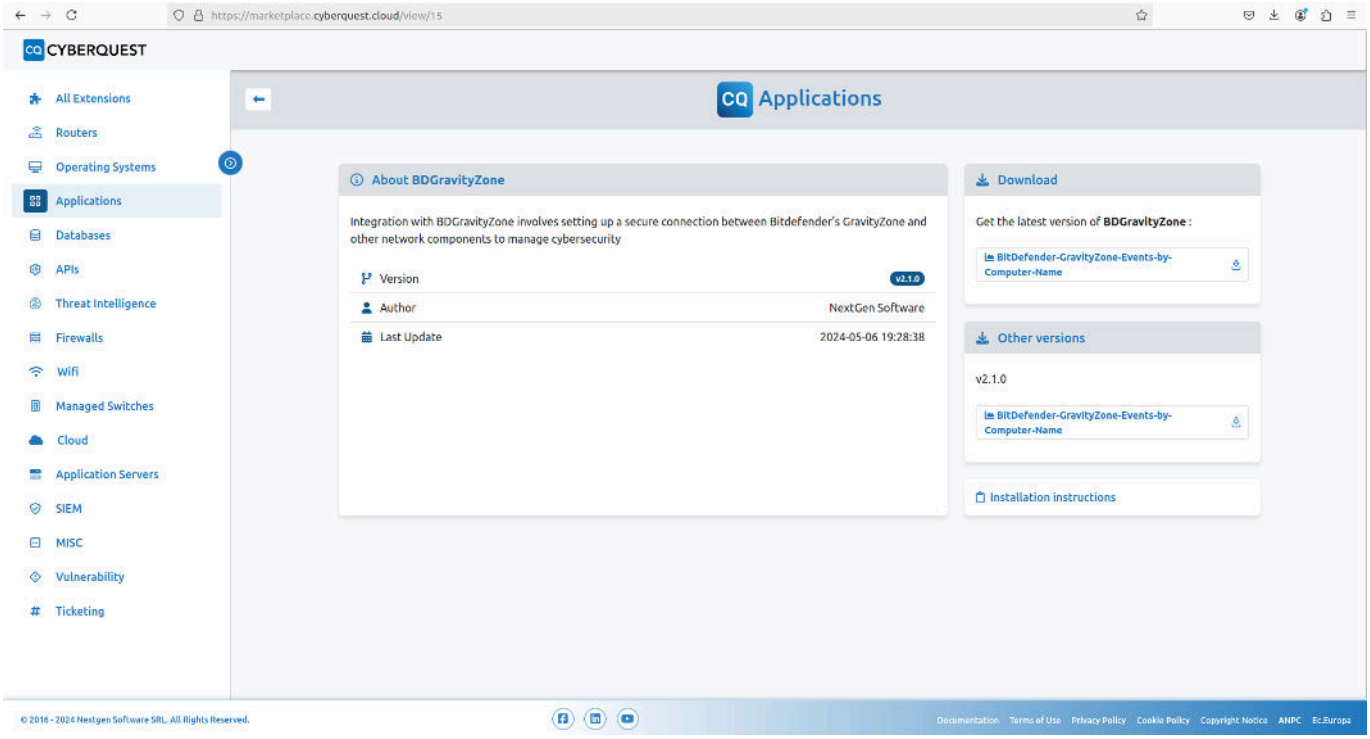


3.**Select Extension for Download**

Locate the specific extension to export. Click the



button to open the extension details page with additional information and download options.

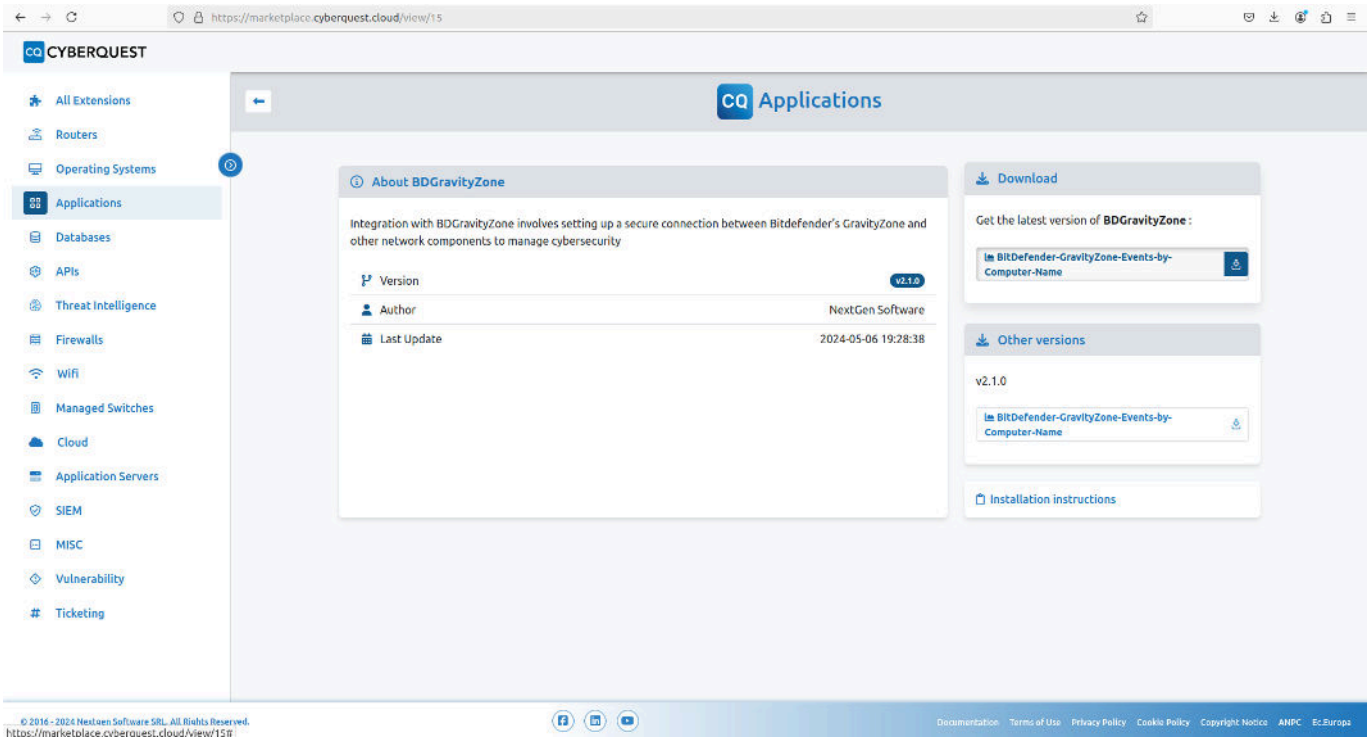


4.**Download the Extension File**

Extensions are packaged in **.cqo file format** (CYBERQUEST object files). Click

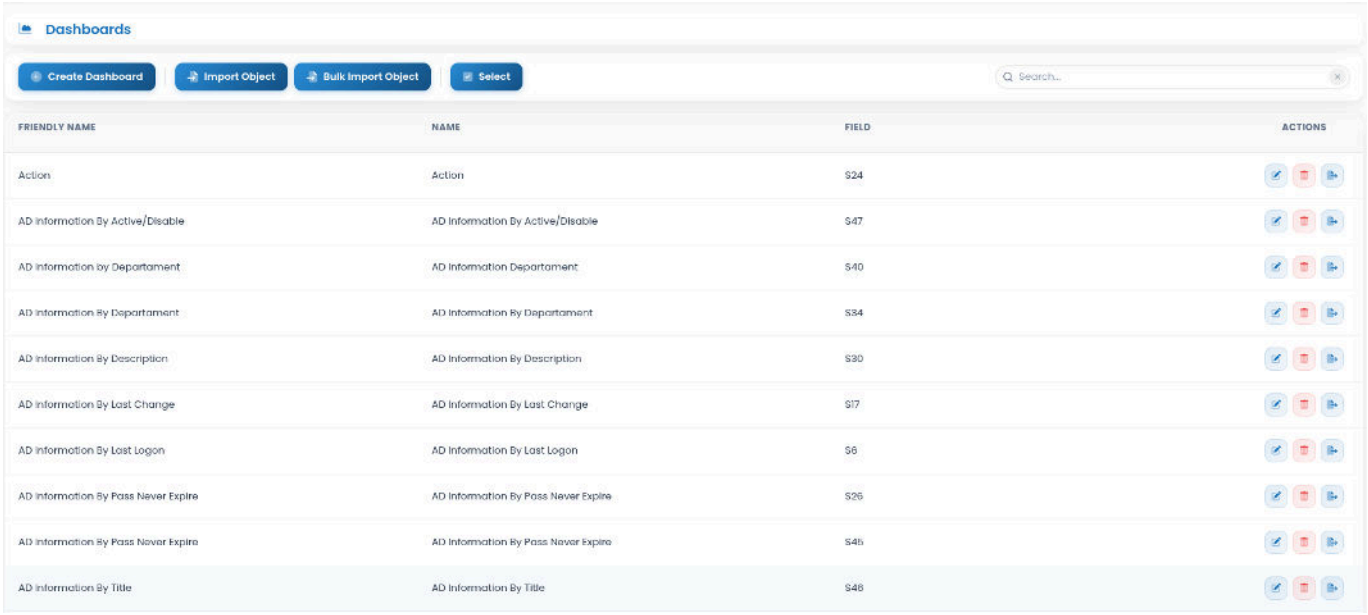


the download button to save the .cqo file to a local machine.



5.Open a web browser and access the CYBERQUEST web interface by entering the application's address or DNS name. The default address for the Web Interface is `https://CyberquestIPAddress` (example).How to import extensions from CYBERQUEST web interface

Navigate to **Settings > Management > Dashboards** to view all objects in the CYBERQUEST instance.



To import the object definition, click



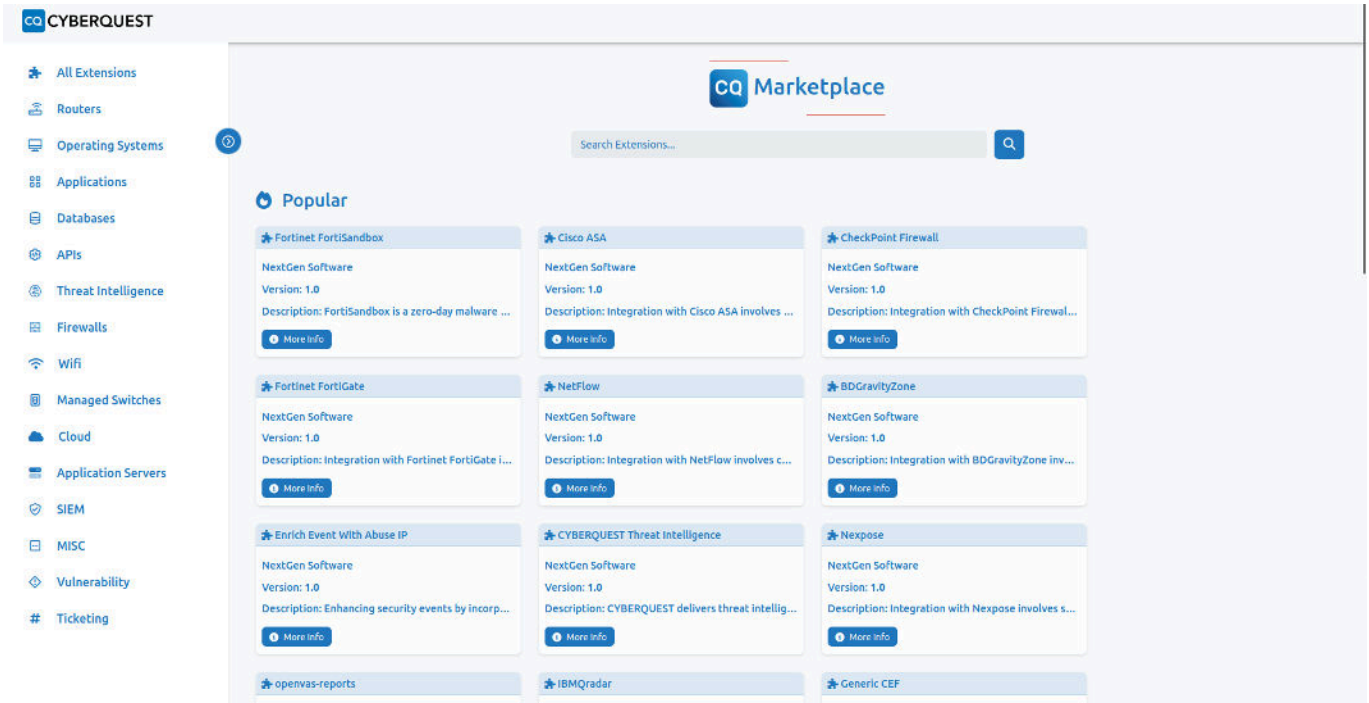
the button and select the .cqo file downloaded from the Marketplace.

How to import extensions from Marketplace cloud

Open a web browser and go to the CYBERQUEST instance by entering its IP address or DNS name. By default, the address looks like ***https://CyberquestIPAddress***.

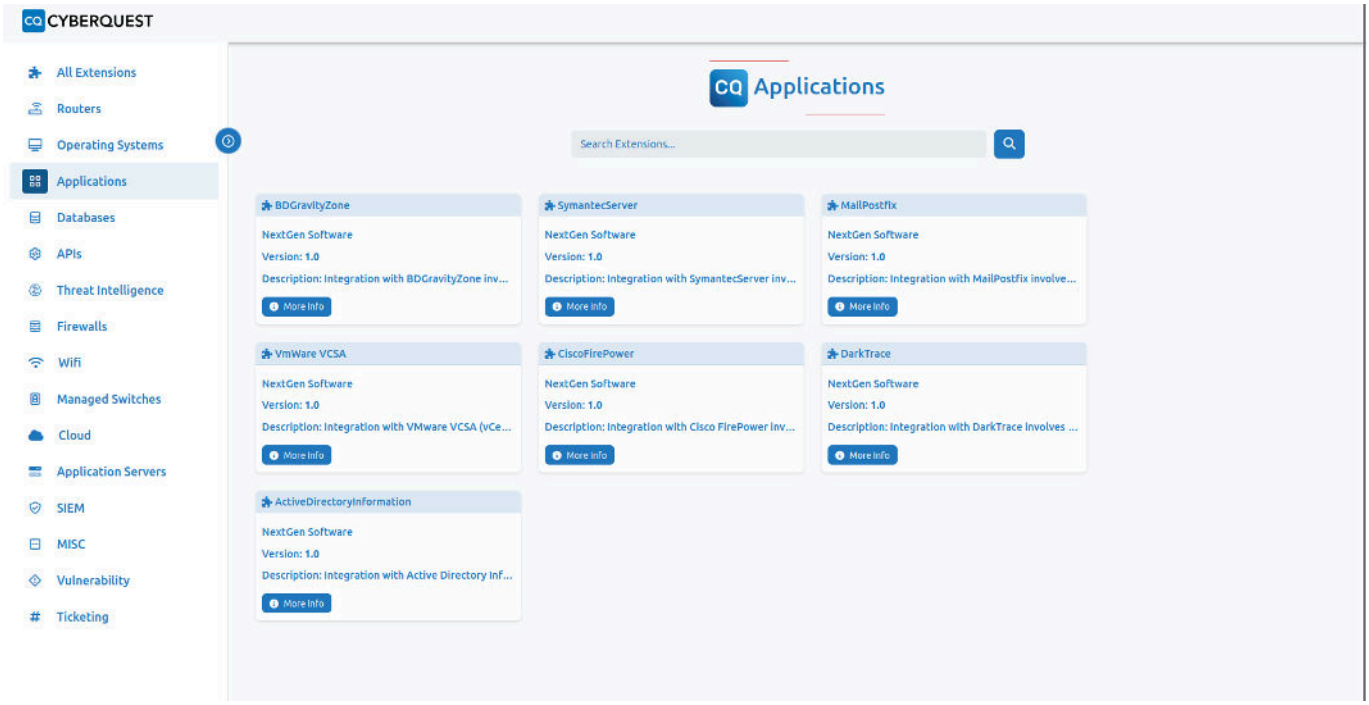
1.**Navigate to Marketplace Settings**

In the CYBERQUEST web interface, go to **Settings > Application Settings > Marketplace**. This section displays all extensions available for installation in your CYBERQUEST instance.



2.**Access Extensions Menu**

From the left-side menu, select the **Extensions** option to view available extensions and import options.

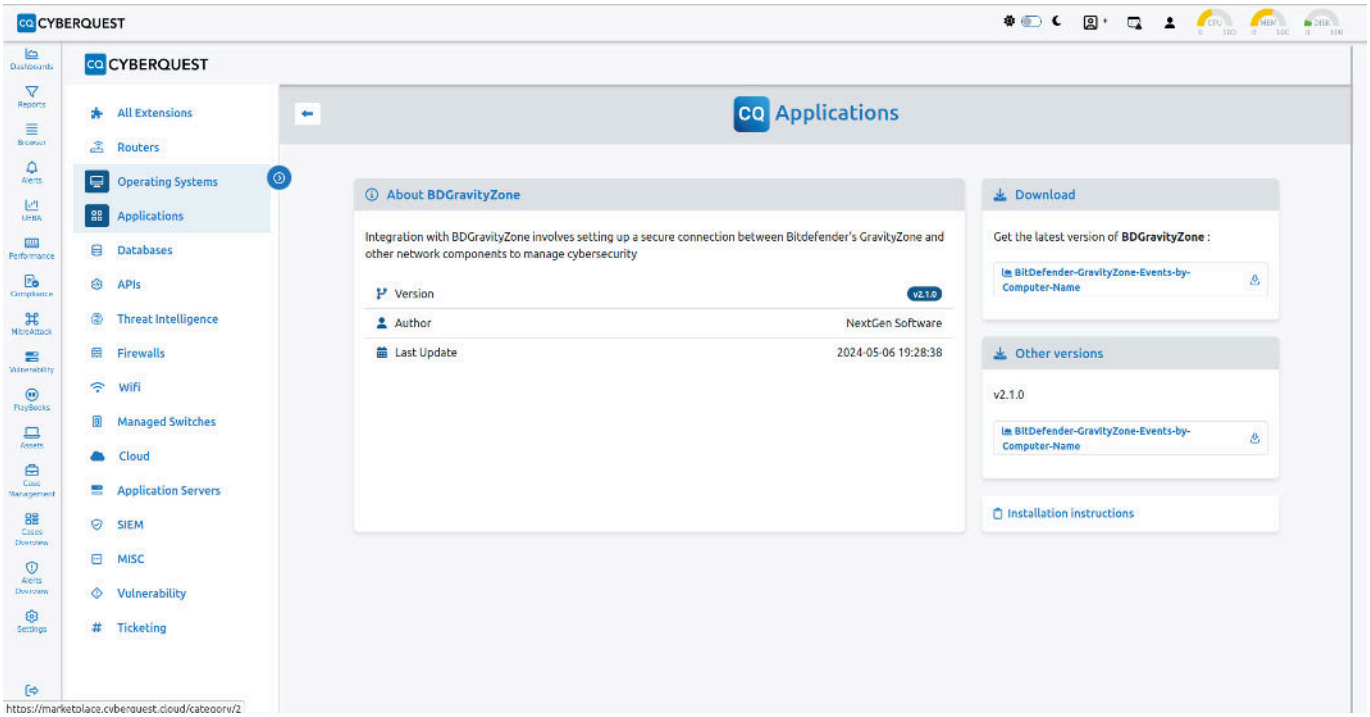


3.**Initiate Extension Installation**

Locate the specific extension to import. Click the



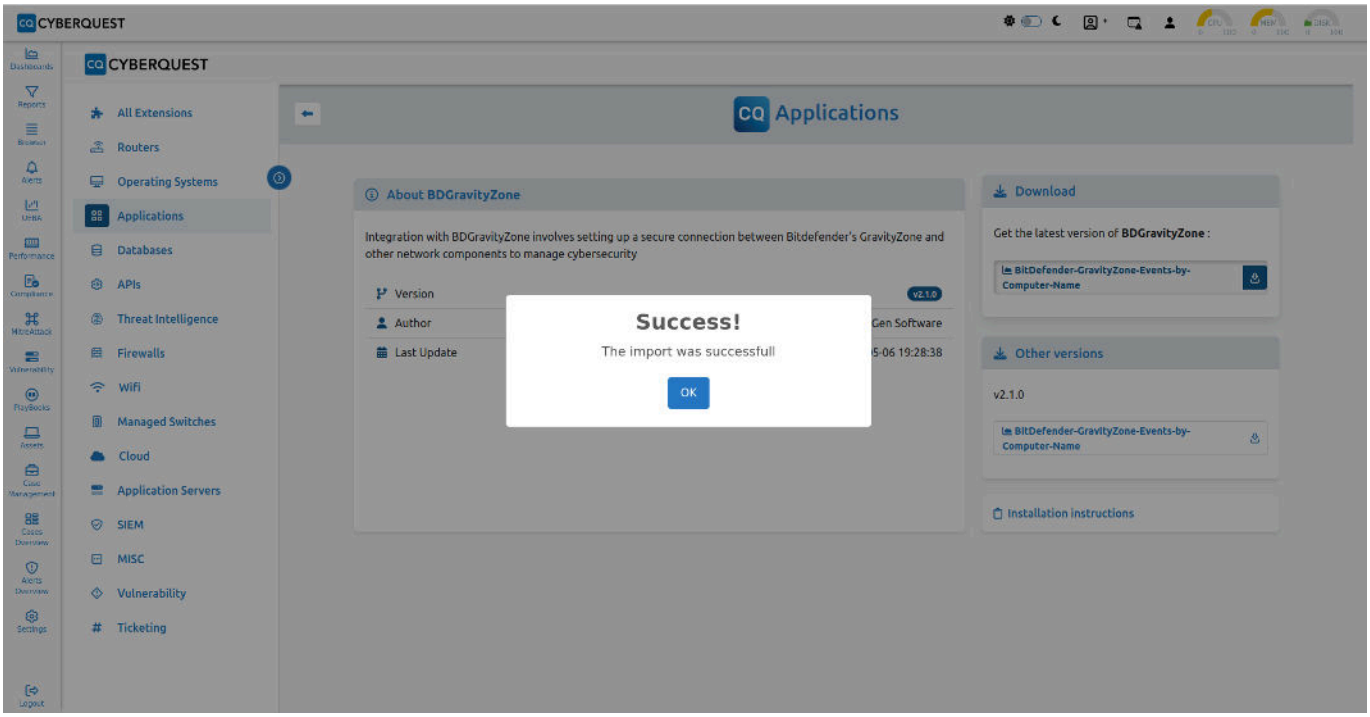
to open the extension details page with additional information and install options.



4.To install the dashboard which is in .cqo file format click

button and the dashboard will be automatically imported in CYBERQUEST.

5.Once the upload process is complete, a success confirmation message appears. The extension will now be available and visible in the appropriate sections of the CYBERQUEST instance.


CYBERQUEST
CYBERQUEST
All Extensions
Routers
Operating Systems
Applications
Databases
APIs
Threat Intelligence
Firewalls
Wifi
Managed Switches
Cloud
Application Servers
SIEM
MISC
Vulnerability
Ticketing
Applications
About BDGravityZone
Integration with BDGravityZone involves setting up a secure connection between Bitdefender's GravityZone and other network components to manage cybersecurity
Version
v2.1.0
Author
Gen Software
Last Update
5-06 19:28:38
Success!
The import was successfull
OK
Download
Get the latest version of BDGravityZone :
BitDefender-GravityZone-Events-by-Computer-Name
Other versions
v2.1.0
BitDefender-GravityZone-Events-by-Computer-Name
Installation instructions

CYBERQUEST API

The script runtime exposes the `CQ` object. The documented namespaces in this section are `Actions`, `Collectors`, `Communications`, `DataSources`, `Integrations`, `Internals`, `Parsers`, and `Utils`.

The remaining properties declared by the runtime are:

- `CQ.ANOMALY_STRING_SPLIT`
- `CQ.DropEvent(Event)`
- `CQ.GenericCredential`, `CQ.GenericSettings`, `CQ.Networks`, and `CQ.Cache`
- `CQ.Test.DefaultParser` and `CQ.Test.ExternalAPIHashmap`
- `CQ.Case` and `CQ.sleep(milliseconds)`

Only use the names and casing shown here; they mirror the declarations in the runtime API.

Collectors

Overview

The `CQ.Collectors` namespace provides collectors for use in customizable CYBERQUEST scripts, including Data Transformation Service (DTS), alerts, and Data Source Manager scripts.

Available members

Access path	Exported collector
`CQ.Collectors.ElasticSearchCollector`	`ElasticSearchCollector`
`CQ.Collectors.CloudTrailCollector`	`CloudTrailCollector`
`CQ.Collectors.CyberQuestIPDataCollector`	`CyberQuestIPDataCollector`
`CQ.Collectors.HttpServerCollector`	`HttpServerCollector`
`CQ.Collectors.CloudGravityZone`	`CloudGravityZone`
`CQ.Collectors.SamsungKnoxCollector`	`SamsungKnoxCollector`
`CQ.Collectors.Office365Collector`	`Office365Collector`
`CQ.Collectors.NucleonCollector`	`NucleonCollector`
`CQ.Collectors.DekeneasOrangeRoCollector`	`DekeneasOrangeRoCollector`

Usage

CyberQuestIPDataCollector

Helper class with the role of contacting `getIpData` api for obtaining data. Extends `BaseCollector` class.

For each event, the module will call a callback received, passing the event back.

Parameters

Parameter	Type	Default	Description
`ipDataUrl`	string	CYBERQUEST IP data service URL	URL to which the collector sends its POST request.

Usage

```
var callBackFunction = function (IP) {
    console.log("BlackListedIP", IP);
};
var parameters = {
    ipDataUrl: "https://example.com/api/getIPData"
};
var Collector = CQ.Collectors.CyberQuestIPDataCollector;
var collector = new Collector(parameters);
collector.execute(callBackFunction);
```

`execute(callbackFunction)` passes the parsed service response to the callback when the HTTP request succeeds. The method does not return the collected value.

ElasticSearchCollector

Connects to the Online DataStorage service. It can collect data from it and has the option of obtaining data in `batch` through the same call. Extends `BaseCollector` class.

On execution, it can receive a callback after each result. Treats the errors received.

Parameters

Parameter	Type	Default	Description
`withCredentials`	boolean	`false`	Enables credentials on HTTP requests.
`auth`	object or string	Empty username and password	HTTP authentication settings. An object has `username` and `password`; a managed-credential GUID may also be used.
`rejectUnauthorized`	boolean	`false`	Controls TLS certificate verification.
`debugLog`	boolean	`false`	Enables collector debug logging.
`elasticSearchUrl`	string	`http://127.0.0.1`	Elasticsearch base URL, without the port or query path.
`elasticSearchQueryUrl`	string	`el_logs_current/_search`	Index and search endpoint appended to the base URL.
`elasticSearchPort`	number	`9200`	Elasticsearch port.
`elasticSearchScrollTimeSpan`	string	`15m`	Scroll retention value sent on the initial request.
`lastLocalTime`	string	`2019-01-01 00:00:00.000`	Initial local-time marker. The collector does not automatically insert it into a custom `searchRequest`.
`searchRequest`	object	Built-in query	Elasticsearch request body. It contains the batch `size`, `sort`, and `query`.

Usage

```
var callBackFunction = function (Event) {
    console.log(Event);
};
var parameters = {
    elasticSearchUrl: "http://192.168.0.1",
    elasticSearchQueryUrl: "logstash*/_search",
    elasticSearchPort: 9200,
    elasticSearchScrollTimeSpan: "1m",
    lastLocalTime: "lastLocalTime",
    searchRequest: {
        "size": 3,
        "sort": [
            { "@timestamp": { "order": "asc" } }
        ],
        "query": {
            "bool": {
                "must": {
                    "match_all": {}
                },
                "filter": [
                    {
                        "range": {
                            "@timestamp": {
                                "gt": lastLocalTime
                            }
                        }
                    }
                ]
            }
        }
    }
};
var collector = CQ.Collectors.ElasticSearchCollector;
collector.init(parameters);
collector.execute(callBackFunction);
```

`init(parameters)` stores the merged collector configuration and returns `undefined`. `execute(callbackFunction)` invokes the callback for every collected hit and returns `undefined`.

CloudTrailCollector

Reads the current CloudTrail file from the CYBERQUEST runtime and invokes the callback once for every item in its `Records` array.

This collector has no configuration parameters. Call `execute(callbackFunction)`, where `callbackFunction` receives one CloudTrail record. The method returns `null` for invalid input or a file without a `Records` array; otherwise, it returns `undefined`.

Usage

```
var collector = new CQ.Collectors.CloudTrailCollector();

collector.execute(function (record) {
    console.log(record);
});
```

HttpServerCollector

Creates an HTTP or HTTPS server. Pass the parameters to the collector constructor, then call `start()`.

Parameters

Parameter	Type	Default	Description
`hostname`	string	`127.0.0.1`	Interface or hostname on which the server listens.
`port`	number	`8080`	Listening port.
`timeout`	number	`60000`	Request timeout in milliseconds.
`routes`	array	`[]`	Route definitions. Each route can contain `path`, `handler`, and HTTP `method`.
`headers`	object	`{}`	Response headers.
`isHTTPS`	boolean	`false`	Creates an HTTPS server when `true`.
`authorization_string`	string	Basic authentication value	Expected value of the `Authorization` header.
`secure`	object	Empty values	TLS configuration containing `key`, `cert`, and `passphrase`.

```
var HttpServerCollector = CQ.Collectors.HttpServerCollector;
var collector = new HttpServerCollector({
    hostname: "127.0.0.1",
    port: 8080,
    routes: [{
        path: "/events",
        method: "POST",
        handler: function (payload) {
            console.log(payload);
        }
    }]
});
collector.start();
```

`start()` starts the underlying server and returns `undefined`.

CloudGravityZone

Starts an HTTP(S) receiver and configures a Bitdefender GravityZone push-event subscription. Create the collector with optional defaults, then pass the server and subscription settings to `execute(serverParams)`.

Collector parameters

Parameter	Type	Default	Description
`CloudGravityZoneURL`	string	GravityZone push JSON-RPC endpoint	Endpoint used to test and enable push-event settings.
`id`	string	Generated UUID	JSON-RPC request ID.
`subscribeToEventTypes`	object	All supported event types enabled	Map of GravityZone event type names to booleans.
`hostname`	string	`localhost`	Default receiver hostname.
`port`	number	`9001`	Default receiver port.
`isHTTPS`	boolean	`false`	Default receiver protocol.
`routes`	array	POST route at `/`	Default receiver routes.

`execute(serverParams)` parameters

`serverParams` accepts the `HttpServerCollector` parameters and the following subscription settings:

Parameter	Type	Description
`register_hostname`	string	Public hostname registered with GravityZone. Subscription setup occurs only when this and `port` are present.
`id`	string	GravityZone API client ID, sent using Basic authorization.
`authorization`	string	Authorization value GravityZone sends to the receiver.
`subscribeToEventTypes`	object	Event-type boolean map overriding the default subscription set.
`requireValidSslCertificate`	boolean	Whether GravityZone must validate the receiver certificate. Defaults to `false`.

Supported keys in `subscribeToEventTypes` are `modules`, `sva`, `registration`, `supa-update-status`, `av`, `aph`, `fw`, `avc`, `uc`, `dp`, `sva-load`, `task-status`, `exchange-malware`, `network-sandboxing`, `adcloud`, `exchange-user-credentials`, `endpoint-moved-out`, `endpoint-moved-in`, `troubleshooting-activity`, `uninstall`, `install`, `hwid-change`, `new-incident`, `antiexploit`, `network-monitor`, `ransomware-mitigation`, and `security-container-update-available`.

`execute(serverParams)` starts the receiver and performs subscription setup when the required registration values are present. It does not return a collected event; receiver routes process incoming payloads through callbacks.

Usage

```
var collector = new CQ.Collectors.CloudGravityZone();

collector.execute({
    hostname: "0.0.0.0",
    port: 9001,
    register_hostname: "events.example.com",
    id: "gravityzone-api-client-id",
    authorization: "receiver-authorization-value",
    requireValidSslCertificate: true
});
```

When no `routes` are supplied, the collector adds a POST route at `/` that converts incoming GravityZone events into CYBERQUEST log records.

SamsungKnoxCollector

Collects Samsung Knox activity logs. Pass overrides to the constructor.

Parameters

Parameter	Type	Description
`apiMasterPoint`	string	Knox API base URL.
`authEndPoint`	string	Access-token endpoint path.
`activityLog`	string	Activity-list endpoint path.
`detailedLog`	string	Detailed-log endpoint path.
`validityForAccessTokenInMinutes`	number	Requested access-token lifetime. Defaults to `30`.
`headers`	object	HTTP headers; defaults to JSON content type.
`keys`	object	RSA certificate data with `Private`, `Public`, and `Identifier` fields.
`clientInfo`	object	Client data containing `clientID`.
`signOptions`	object	JWT options containing `audience`, `expiresIn`, and `algorithm`; `jwtid` is generated by the collector.
`request`	object	Activity-list request containing `pageNum`, `pageSize`, and `filter`. The default filter has a `duration` of 15.

Supply your own Knox credentials and RSA keys; do not expose them in scripts or documentation.

Call `execute(callbackFunction)`. The callback receives each normalized Knox record. The method returns the number of records retrieved.

Usage

```
var collector = new CQ.Collectors.SamsungKnoxCollector({
    keys: {
        Private: "base64-encoded-private-key",
        Public: "base64-encoded-public-key",
        Identifier: "certificate-identifier"
    },
    clientInfo: {
        clientID: "knox-client-identifier"
    },
    request: {
        pageNum: 0,
        pageSize: 100,
        filter: {
            duration: 15
        }
    }
});

var recordCount = collector.execute(function (record) {
    console.log(record);
});
console.log("Collected records:", recordCount);
```

Office365Collector

Collects Microsoft 365 Management Activity API content.

Parameters

Parameter	Type	Required	Description
`tenant_id`	string	Yes	Microsoft Entra tenant ID.
`client_id`	string	Yes	Application client ID.
`client_secret`	string	Yes	Application client secret.
`headers`	object	No	Additional HTTP headers.
`logs`	array	No	Content types to collect. Defaults to `Audit.Exchange`, `Audit.Sharepoint`, and `Audit.AzureActiveDirectory`.
`lastLocalTime`	string	No	Start time in `YYYY-MM-DDTHH:mm:ss.SSSZ` form. If omitted, collection starts five hours before the current time.
`localTS`	number	No	Unix timestamp used for emitted records when supplied.

Call `execute(callbackFunction)`. The callback receives each normalized event and an optional `localTS` value. The method returns an object containing `count` (the sum of callback return values) and `lastLocalTime`. It returns `null` when required credentials are absent and may return `undefined` if authentication fails.

Usage

```
var collector = new CQ.Collectors.Office365Collector({
    tenant_id: "microsoft-entra-tenant-id",
    client_id: "application-client-id",
    client_secret: "application-client-secret",
    logs: [
        "Audit.Exchange",
        "Audit.Sharepoint",
        "Audit.AzureActiveDirectory"
    ],
    lastLocalTime: "2026-07-27T00:00:00.000Z"
});

var result = collector.execute(function (event, localTS) {
    console.log(event, localTS);
    return 1;
});
console.log(result);
```

NucleonCollector

Provides Nucleon/CyberCure threat-intelligence endpoints. Pass overrides to the constructor.

Parameters

Parameter	Type	Description
`ClientName`	string	Nucleon client name.
`clientID`	string	Nucleon client ID.
`search`	object	Search settings: `searchURL`, `basicAuthCredentials` (`username` and `password`), and `Usrn`.
`feedUrl`	string	CyberCure feed base URL.
`customHeaders`	object	Request headers. Defaults to form-encoded content and JSON response.
`activeThreats`	object	Active-threat settings: `url` and `credentials` (`cid` and `user`).

`getActiveThreats(callbackFunction)` invokes the callback for every returned threat and returns `undefined`. `executeActiveThreats(body)` accepts a form body object and returns the parsed response, or `null` when the request fails or cannot be parsed.

Usage

```
var collector = new CQ.Collectors.NucleonCollector();

collector.getActiveThreats(function (threat) {
    console.log(threat);
});
```

DekeneasOrangeRoCollector

Collects threat-intelligence data from the Dekeneas API. Pass overrides to the constructor.

Parameters

Parameter	Type	Description
`ipDataUrl`	string	Dekeneas API endpoint.
`content`	object	Form fields containing `apikey`, `fetch`, and `period`. `fetch` supports `darknet`, `generic`, `iot`, or `all`; `period` supports day, week, and month values such as `1d`, `1w`, and `1m`.

Call `execute(callbackFunction)`. If the callback is omitted, the collector creates CYBERQUEST log records through its built-in callback. The method returns `undefined`.

Usage

```
var collector = new CQ.Collectors.DekeneasOrangeRoCollector({
    ipDataUrl: "https://example.com/api",
    content: {
        apikey: "dekeneas-api-key",
        fetch: "all",
        period: "1d"
    }
});

collector.execute(function (event) {
    console.log(event);
});
```

Communications

Overview

The `CQ.Communications` namespace provides HTTP and notification helpers for use in customizable CYBERQUEST scripts, including Data Transformation Service (DTS) and alert scripts.

Available members

Access path	Exported member
`CQ.Communications.HttpRequest`	`HttpRequest`
`CQ.Communications.sendMessage`	`sendMessage`

HttpRequest

This class is a wrapper that encapsulates the http client on specific targets (windowsagent, etc.).

All methods that send requests will return a uniform formatted response, along with the status code or potential errors.

Access this class through the global `CQ` object as `CQ.Communications.HttpRequest`.

Configuration

```
const config = {
  method: "GET",
  data: null,
  withCredentials: false,
  CredentialsType: "plain", // "plain", "encrypted", or "managed"
  timeout: 60000, // milliseconds
  rejectUnauthorized: false,
  auth: {
    username: "user",
    password: "pass"
  },
  headers: {},
  cookies: [],
  responseSizeLimit: -1 // unlimited
};
```

These are the defaults applied by `HttpRequest`. The `auth` value may also be a managed-credential GUID. Request-specific configuration is merged with these defaults. The convenience methods override `method` and, where applicable, `data` before sending the request.

Request methods

Method	Parameters	Returns
`get(url, config = null)`	Request URL and optional configuration object.	`HttpResponse`
`post(url, data, config = null)`	Request URL, request body, and optional configuration.	`HttpResponse`
`put(url, data, config = null)`	Request URL, request body, and optional configuration.	`HttpResponse`
`delete(url, config = null)`	Request URL and optional configuration.	`HttpResponse`
`head(url, config = null)`	Request URL and optional configuration.	`HttpResponse`
`putV2(url, data, config = null)`	Request URL, request body, and optional configuration.	`HttpResponse`
`deleteV2(url, data, config = null)`	Request URL, request body, and optional configuration.	`HttpResponse`
`headV2(url, data, config = null)`	Request URL, request body, and optional configuration.	`HttpResponse`
`patchV2(url, data, config = null)`	Request URL, request body, and optional configuration.	`HttpResponse`

The V2 variants pass `data` through to the runtime transport for HTTP methods whose original wrapper does not accept a request body.

`HttpRequest.get`

```
CQ.Communications.HttpRequest.get(url, config=null)
```

- **HttpResponse**

`HttpRequest.post`

```
CQ.Communications.HttpRequest.post(url, data, config=null)
```

- **HttpResponse**

`HttpRequest.put`

```
CQ.Communications.HttpRequest.put(url, data, config=null)
```

- **HttpResponse**

`HttpRequest.delete`

```
CQ.Communications.HttpRequest.delete(url, config=null)
```

- **HttpResponse**

`HttpRequest.head`

```
CQ.Communications.HttpRequest.head(url, config=null)
```

- **HttpResponse**

`HttpRequest.putV2`

```
CQ.Communications.HttpRequest.putV2(url, data, config=null)
```

`HttpRequest.deleteV2`

```
CQ.Communications.HttpRequest.deleteV2(url, data, config=null)
```

`HttpRequest.headV2`

```
CQ.Communications.HttpRequest.headV2(url, data, config=null)
```

`HttpRequest.patchV2`

```
CQ.Communications.HttpRequest.patchV2(url, data, config=null)
```

`HttpResponse`

Properties:

- int **statusCode**
- string **data** - The raw response body
- string **header** - The raw response header
- Array **headers** - The response headers
- string **errorMsg** - Error message, if any
- string **contentType** - Response content type
- boolean **isError** - Whether the request failed
- int **messageLength** - Response-body length

`HttpResponse.getData()`

Returns the response body stored in `data` without parsing it.

`HttpResponse.asJson()`

Returns the parsed response body when it contains valid JSON; otherwise, returns `null`.

`HttpResponse.asXml()`

Returns the parsed response body when it contains valid XML; otherwise, returns `null`.

Attributes are kept with the `@_` prefix, element text that sits next to attributes is under `#text`, and repeated elements become an array. For example, `<host name="srv1">up</host>` becomes `{host: {"@_name": "srv1", "#text": "up"}}`.

`sendMessage`

Parameters:

- **text** - this is the message of the notification
- **type** - what platform the notification is sent to (`email` by default, can be sent to `slack` or `teams` as well)
- **additionalParamateres** (`url`, `subjectData`, and `to` are optional at this layer)

Taking into account the `type` parameter of the `sendMessage` method, the module will select the appropriate particular class, instantiate it under its own rules and dispatch the notification.

Usage

```
CQ.Communications.sendMessage(message, platform, {
  url: "",
  to: "optional",
  subjectData: "optional"
})
```

Parameter	Type	Default	Description
`text`	string	Required	Notification message.
`type`	string	`"email"`	One of `"email"`, `"slack"`, or `"teams"`.
`additionalParamateres`	object	Object with `url`, `subjectData`, and `to` set to `null`	Delivery-specific options.
`additionalParamateres.url`	string or null	`null`	Destination hook URL.
`additionalParamateres.subjectData`	any	`null`	Optional subject data.
`additionalParamateres.to`	string or null	`null`	Email recipient.

`subjectData` is accepted for compatibility but is not currently used by the runtime notification dispatcher. `url` is passed to the selected notification hook; whether it is required depends on that hook. For email, the dispatcher constructs this payload before calling the email hook:

```
{
  payload: {
    data: {
      to: additionalParamateres.to,
      Severity: 4,
      Message: text
    }
  },
  localTime: moment().unix()
}
```

Slack and Teams receive a message object containing `{ text }` instead; the hook determines how `url` is used. The function returns the selected hook's `sendMessage` result, or `undefined` when `type` is unsupported.

DataSources

Overview

The `CQ.DataSources` namespace provides data-source helpers for use in customizable CYBERQUEST scripts, including Data Transformation Service (DTS) and alert scripts.

Available members

Access path	Exported class
`CQ.DataSources.DataSourceStatus`	`DataSourceStatus`

DataSourceStatus

This object reads and adjusts the last local-time marker for the current data source. The timestamp methods use different units as indicated below:

Method	Parameters	Returns
`getLastLocalTimeAsUTCAsTimeStampMilliseconds()`	None.	UTC timestamp in **milliseconds**.
`getLastLocalTimeUTCTimeStampSeconds()`	None.	UTC timestamp in **seconds**.
`getLastLocalTimeStamp()`	None.	Last local timestamp in **seconds**.
`addSecondsToLastLocalTime(seconds)`	`seconds` (number): offset to add.	`undefined`; updates the runtime marker in place.
`getLastLocalTimeFormatted()`	None.	String formatted as `YYYY-MM-DD HH:mm:ss.SSS`, based on the marker in **milliseconds**.

`getLastLocalTimeAsUTCAsTimeStampMilliseconds()` and `getLastLocalTimeUTCTimeStampSeconds()` represent the same UTC marker in different units. `getLastLocalTimeStamp()` returns the local marker in seconds; use `getLastLocalTimeFormatted()` when a formatted local-time string is needed.

Internals

Overview

The `CQ.Internals` namespace provides encryption helpers for use in customizable CYBERQUEST scripts, including Data Transformation Service (DTS) and alert scripts. CYBERQUEST uses AES-256 encryption for passwords.

Available members

Access path	Exported function
`CQ.Internals.encrypt`	`Encryption.encrypt`
`CQ.Internals.decrypt`	`Encryption.decrypt`

Usage

`encrypt`

```
CQ.Internals.encrypt(clearTxtValue);
```

Parameter	Type	Description
`clearTxtValue`	string	Clear-text value to encrypt.

Returns the encrypted value produced by the runtime encryption target.

`decrypt`

```
CQ.Internals.decrypt(encryptedValue);
```

Parameter	Type	Description
`encryptedValue`	string	Encrypted value to decrypt.

Returns the decrypted value produced by the runtime encryption target.

Parsers

Overview

The `CQ.Parsers` namespace provides parsing utilities for use in customizable CYBERQUEST scripts, including Data Transformation Service (DTS) and alert scripts.

Available members

Access path	Exported utility
`CQ.Parsers.fast_xml_parser`	`fast_xml_parser`
`CQ.Parsers.string2Bytes`	`bytes`
`CQ.Parsers.urlParse`	`urlParse`
`CQ.Parsers.csvjson`	`csvjson`
`CQ.Parsers.getObjectFromDirtyJsonString`	`getObjectFromDirtyJsonString`

Usage

fast_xml_parser

Validate XML, Parse XML to JS/JSON and vice versa, or parse XML to Nimn rapidly without C/C++ based libraries and no callback.

Access the package as `CQ.Parsers.fast_xml_parser`.

```
const xml = "<event><id>42</id></event>";

const validation = CQ.Parsers.fast_xml_parser.validate(xml);
const event = CQ.Parsers.fast_xml_parser.parse(xml);
```

`validate(xml)` reports whether an XML string is valid. `parse(xml, options)` returns the parsed JavaScript value; pass parser options as the optional second argument.

Method	Parameters	Returns
`validate(xml)`	`xml` (string).	Validation result from `fast-xml-parser`.
`parse(xml, options)`	XML string and optional parser-options object.	Parsed JavaScript value.

For more information on `fast_xml_parser` click **here** (https://www.npmjs.com/package/fast-xml-parser).

string2Bytes

Utility to parse a string bytes (ex: 1TB) to bytes (1099511627776) and vice-versa.

Access it as `CQ.Parsers.string2Bytes`.

```
const bytes = CQ.Parsers.string2Bytes("1TB");
const displayValue = CQ.Parsers.string2Bytes.format(bytes);
```

Call the utility with a size string to obtain a byte count. Use `.format(bytes)` to produce a readable size string.

Call	Parameters	Returns
`string2Bytes(value)`	Human-readable size string such as `"1TB"`.	Numeric byte count, or the package's invalid-input result.
`string2Bytes.format(value, options)`	Byte count and optional formatting options.	Human-readable size string.

For more information on `bytes` click **here** (https://www.npmjs.com/package/bytes).

urlParse

Parse a URL with `CQ.Parsers.urlParse`:

```
const parsedUrl = CQ.Parsers.urlParse("https://example.com:8443/path?source=api");

parsedUrl.hostname; // "example.com"
parsedUrl.port;     // "8443"
parsedUrl.pathname; // "/path"
```

The first parameter is the URL string or URL-like value. Package-supported optional parameters may provide a base URL and parsing behavior. The call returns a parsed URL object.

For more information on `urlParse` click **here** (https://www.npmjs.com/package/url-parse).

csvjson

CSV conversion helpers are available as `CQ.Parsers.csvjson`.

```
const rows = CQ.Parsers.csvjson.toObject("name,score\nAda,10");
const csv = CQ.Parsers.csvjson.toCSV(rows);
```

Method	Parameters	Returns
`toObject(csv, options)`	CSV string and optional conversion settings.	Array of row objects.
`toCSV(rows, options)`	Array of objects and optional conversion settings.	CSV string.

For more information on `csvjson`, click **here** (https://github.com/pradeep-mishra/csvjson).

getObjectFromDirtyJsonString

Extracts a JSON object from a string that contains surrounding non-JSON text. It returns `null` when no object can be extracted.

```
const value = CQ.Parsers.getObjectFromDirtyJsonString(
  "Remote response: {\"status\": \"ok\"}"
);
```

The function accepts one string and returns the extracted object. It returns `null` when it cannot extract an object.

For more information on `getObjectFromDirtyJsonString`, click **here** (https://github.com/esoodev/extract-json-string).

Utilities

Overview

The `CQ.Utils` namespace provides general utilities for use in customizable CYBERQUEST scripts, including Data Transformation Service (DTS) and alert scripts.

Available members

Access path	Exported utility
`CQ.Utils.moment`	`moment`
`CQ.Utils.recursiveCleanupObjectProperties`	`recursiveCleanupObjectProperties`
`CQ.Utils.LocalStorage`	`LocalStorage`
`CQ.Utils.CQDataBase`	`CQDataBase`

moment

This object manipulates date and time related information. Click this **link** (https://momentjs.com/) for more information.

Call `CQ.Utils.moment()` with no arguments for the current time, or pass a supported date value and optional format. It returns a Moment object.

recursiveCleanupObjectProperties

This method takes an object and recursively goes through all the objects or arrays that it contains, renaming all the keys such that the `@` and `:` symbols are replaced with `_`. This way, the keys will present a cleaner format.

Parameters: **inputObject**

Usage:

```
CQ.Utils.recursiveCleanupObjectProperties(inputText);
```

Returns the cleaned object. Nested objects and arrays are processed recursively.

LocalStorage

The class is designed to make temporary data persist. It also acts as a caching module. (key->value)

set

Keeps a value in the local storage under a certain key. Optionally, expiring time can be specified in seconds.

Parameters:

- **listName**
- **name**
- **value**
- **ttl** (900 by default, -1 is indefinitely)

Usage:

```
CQ.Utils.LocalStorage.set(listName, keyName, value);
```

Returns the runtime storage target's result. Returns `false` when either name is missing or shorter than two characters, when `value` is `null`, or when `ttl` is not a finite number.

get

Returns a stored value. If the value does not exist, it will return an empty object in order to simplify the validation checks.

Parameters:

- **listName**
- **name**

Usage:

```
CQ.Utils.LocalStorage.get(listName, keyName);
```

Returns the stored value. Returns `{}` for invalid names, missing data, or storage errors.

erase

Deletes a single value from the local storage.

Parameters:

- **listName**
- **name**

Usage:

```
CQ.Utils.LocalStorage.erase(listName, keyName);
```

Returns `undefined`.

clear

Deletes all values from the local storage.

Parameters:

- **listName**

Usage:

```
CQ.Utils.LocalStorage.clear(listName);
```

Returns `undefined` after a successful clear, or `false` when the storage target throws an error.

removeKeysStartingWith

Deletes from local storage all values with keys that start with a certain string.

Parameters:

- **listName**
- **name**

Usage:

```
CQ.Utils.LocalStorage.removeKeysStartingWith(listName, name);
```

Returns `undefined` on success, or `false` when the storage target throws an error.

listKeys

```
CQ.Utils.LocalStorage.listKeys(listName);
```

`listName` defaults to `null`. Invalid names return `[]`. The current wrapper does not return the storage target's value for a valid name and therefore returns `undefined`.

listKeysByPattern

```
CQ.Utils.LocalStorage.listKeysByPattern(pattern);
```

Returns the matching keys from the storage target. A missing pattern or a pattern shorter than two characters returns `[]`.

CQDataBase

`CQ.Utils.CQDataBase` provides database helpers for scripts that receive a MySQL connection ID. Its basic data operations are:

```
CQ.Utils.CQDataBase.getData(MySQLConnectionID, tableName, limit, whereClause);
CQ.Utils.CQDataBase.getReportParentID(MySQLConnectionID, parentGUID);
CQ.Utils.CQDataBase.insertData(MySQLConnectionID, tableName, values);
CQ.Utils.CQDataBase.updateData(MySQLConnectionID, tableName, values, whereClause, limit);
CQ.Utils.CQDataBase.deleteData(MySQLConnectionID, tableName, whereClause, limit);
CQ.Utils.CQDataBase.truncateData(MySQLConnectionID, tableName);
```

Database method parameters and returns

Method	Parameters	Defaults	Returns
`getData`	Connection ID, table name, limit, where clause.	`limit = 10000`, `whereClause = ""`	Runtime database target result.
`getReportParentID`	Connection ID and parent GUID.	None.	Matching report ID, or `null`.
`insertData`	Connection ID, table name, values object.	`values = {}`	Runtime database target result.
`updateData`	Connection ID, table name, values, where clause, limit.	`values = {}`, `whereClause = ""`, `limit = 1`	`undefined`
`deleteData`	Connection ID, table name, where clause, limit.	`whereClause = ""`, `limit = 1`	`undefined`
`truncateData`	Connection ID and table name.	None.	Runtime database target result.

Treat table names, where clauses, and values as trusted administrative input. Build where clauses carefully and do not include untrusted text.

Actions

Overview

The `CQ.Actions` namespace provides the `TI` and `SSL` helpers for use in CYBERQUEST scripts.

Available members

Access path	Exported helper
`CQ.Actions.TI`	`TI`
`CQ.Actions.SSL`	`SSL`

Usage

TI

`CQ.Actions.TI` manages Threat Intelligence block lists. Before invoking a TI request, configure the target host and bearer token:

```
CQ.Actions.TI.setHost("https://webapplication");
CQ.Actions.TI.setBearerToken("token");
```

Configuration and helpers

Method	Parameters	Returns
`setHost(value)`	`value` (string): API base URL.	`undefined`
`getHost()`	None.	Configured host string. Throws if it is undefined.
`setBearerToken(value)`	Bearer token string without the `Bearer` prefix.	`undefined`
`validateBearerToken()`	None.	`undefined`. Throws if authentication is missing.
`setBody(data)`	Any JSON-serializable value.	`undefined`
`getOutput(response)`	An `HttpResponse`.	Parsed JSON, or `{}`.
`addSecondsToNow(seconds)`	Number of seconds.	Date-time string formatted as `YYYY-MM-DD HH:mm:ss`.

Threat Intelligence operations

Method	Parameters	Returns
`CheckListInTI(data)`	Object containing `list` and `type`.	Parsed API response, or `{}`.
`CheckAndBlockIP(data, expires, comment, list)`	One value or an array; optional expiration, comment, and list.	Parsed API response, or `{}`.
`GetBlockedIps(list)`	Optional list name.	`IntegrationHTTPResponse` whose `data` is an array of IP entries.
`GetBlockedDomains(list)`	Optional list name.	`IntegrationHTTPResponse` whose `data` is an array of domain entries.
`AddBlockedIps(data, expires, comment, list)`	One value or an array; optional expiration, comment, and list.	Parsed API response, or `{}`.
`AddBlockedDomains(data, expires, comment, list)`	One value or an array; optional expiration, comment, and list.	Parsed API response, or `{}`.
`RemoveBlockedIps(data)`	One IP value or an array.	Parsed API response, or `{}`.
`RemoveBlockedDomains(data)`	One domain value or an array.	Parsed API response, or `{}`.

For add and check-and-block operations, `expires` defaults to `null`, `comment` to `""`, and `list` to `null`. An integer `expires` value is interpreted as seconds from the current time.

SSL

`CQ.Actions.SSL` validates TLS certificates for one or more hosts.

```
CQ.Actions.SSL.validateCertificate(host);
CQ.Actions.SSL.validateCertificates(hosts);
```

Method	Parameters	Returns
`validateCertificate(host)`	`host` (string): hostname to validate.	Result object with `isSuccess` and `data`.
`validateCertificates(hosts)`	`hosts` (array of strings).	`{ isSuccess, data }`, where `data` contains one result per host.

For `validateCertificate`, `data` contains `STDOUT` and `STDERR`. When the certificate expiration can be parsed, it also contains `expiration_date` and `days_difference`. Invalid input returns `{ isSuccess: false, message }`.

Integrations

Overview

The `CQ.Integrations` namespace exposes configured integration objects to CYBERQUEST scripts.

Available members

Access path	Exported object
`CQ.Integrations.NetAlert`	`NetAlert`
`CQ.Integrations.QRadar`	`QRadar`
`CQ.Integrations.IntegrationsNotifications`	`IntegrationsNotifications`
`CQ.Integrations.Ticketing.ServiceNow`	`ServiceNowTicketing`
`CQ.Integrations.Ticketing.ConnectWise`	`ConnectWiseTicketing`
`CQ.Integrations.Ticketing.Remedy`	`RemedyTicketing`

Usage

Access an integration through its complete `CQ.Integrations` path. These exports are already-created objects; do not invoke them with `new`.

```
CQ.Integrations.NetAlert.setHost("https://webapplication");
CQ.Integrations.NetAlert.setBearerToken("token");
```

NetAlert

`CQ.Integrations.NetAlert` queries traffic and alert data. Call `setHost` and `setBearerToken` before making a request.

Configuration methods

Method	Parameters	Returns
`setHost(value)`	`value` (string): API base URL.	`undefined`
`getHost()`	None.	Configured host string. Throws if no host is set.
`setBearerToken(value)`	`value` (string): bearer token without the `Bearer` prefix.	`undefined`
`validateBearerToken()`	None.	`undefined`. Throws if no bearer token is set.
`setBody(data)`	`data` (any JSON-serializable value).	`undefined`
`getOutput(response)`	`response` (`HttpResponse`).	Parsed JSON, or `{}` when unavailable.
`parseFilter(filter)`	`filter` (string).	The supplied non-empty string, otherwise `"*"`.

Query methods

Method	Parameters	Returns
`GetTraffic(data)`	`data.StartDate`, `data.EndDate`, optional `data.Filter`, and `data.maxNumberOfResults`.	Parsed API response, or `{}`.
`GetAlerts(data)`	`data.StartDate`, `data.EndDate`, optional `data.Filter`, and `data.maxNumberOfResults`.	Parsed API response, or `{}`.
`GetSingleTraffic(data)`	`data.Flow_GUID`: flow identifier.	Parsed API response for at most one flow, or `{}`.
`GetSingleAlert(data)`	`data.AlertID`: alert identifier.	Parsed API response for at most one alert, or `{}`.
`GetTrafficCountByField(data)`	Date range, optional filter, `data.Field`, and `data.maxNumberOfResults`.	Parsed API response, or `{}`.
`GetAlertCountByField(data)`	Date range, optional filter, `data.Field`, and `data.maxNumberOfResults`.	Parsed API response, or `{}`.
`GetSrcIPConnections(data)`	Date range, optional filter, and `data.maxNumberOfResults`.	Parsed API response, or `{}`.
`GetDestIPConnections(data)`	Date range, optional filter, and `data.maxNumberOfResults`.	Parsed API response, or `{}`.

```
const alerts = CQ.Integrations.NetAlert.GetAlerts({
  StartDate: "2026-01-01 00:00:00",
  EndDate: "2026-01-02 00:00:00",
  Filter: "SourceIP:192.0.2.10",
  maxNumberOfResults: 100
});
```

QRadar

`CQ.Integrations.QRadar` runs an Ariel query and waits for it to complete.

Method	Parameters	Returns
`setHost(value)`	`value` (string): QRadar base URL.	`undefined`
`getHost()`	None.	Configured host string. Throws if no host is set.
`setBasicAuth(username, password)`	Basic-auth username and password strings.	`undefined`
`validateAuth()`	None.	`undefined`. Throws if authentication is not configured.
`setBody(data)`	`data` (any JSON-serializable value).	`undefined`
`getOutput(response)`	`response` (`HttpResponse`).	Parsed JSON, or `{}`.
`GetData(query_expression)`	`query_expression` (string): Ariel query expression.	`IntegrationHTTPResponse`.

`GetData` returns an object with `isSuccess`, `data`, `message`, and `errorMessage` properties. On success, `data` contains the returned events. The method polls every 15 seconds and blocks until QRadar reports that the search is complete.

```
const result = CQ.Integrations.QRadar.GetData(
  "SELECT * FROM events LAST 10 MINUTES"
);
```

IntegrationsNotifications

`CQ.Integrations.IntegrationsNotifications` inherits common authentication helpers and sends email through the CYBERQUEST notification endpoint.

Authentication methods

Method	Parameters	Returns
`setBearerToken(value)`	Bearer token string without the `Bearer` prefix.	`undefined`
`setBasicAuth(username, password)`	Basic-auth username and password strings.	`undefined`
`disableAuth()`	None.	`undefined`; subsequent calls do not require configured authentication.

`SendEmail`

```
CQ.Integrations.IntegrationsNotifications.SendEmail(
  to,
  subject,
  message,
  host
);
```

Parameter	Type	Default	Description
`to`	string	Required	Email recipient passed to the notification endpoint.
`subject`	string	`""`	Email subject.
`message`	string	`""`	Email body.
`host`	string	`"webapplication"`	Hostname used in the HTTPS endpoint.

Returns an `IntegrationHTTPResponse`. Check its `isSuccess` and `message` properties to determine whether the endpoint accepted the request.

Ticketing

`CQ.Integrations.Ticketing` exposes one ready-to-use object per supported ticketing system: `ServiceNow`, `ConnectWise`, and `Remedy`. All three share the same shape — configure host and credentials, then call `CreateTicket`, which always returns an `IntegrationHTTPResponse` (`isSuccess`, `data`, `message`, `errorMessage`).

```
const ticket = CQ.Integrations.Ticketing.ServiceNow
  .setCredentialsByGUID("00000000-0000-0000-0000-000000000000")
  .setHost("https://yourinstance.service-now.com")
  .CreateTicket({
    summary: Event.AlertName,
    description: Event.Description,
    priority: "2"
  });

if (ticket.isSuccess) {
  Event.S1 = ticket.data.number;
}
```

ServiceNow

Method	Parameters	Returns
`setHost(value)`	`value` (string): ServiceNow instance base URL.	`this`
`getHost()`	None.	Configured host string. Throws if no host is set.
`setBasicAuth(username, password)`	Basic-auth username and password strings.	`this`
`setCredentialsByGUID(guid)`	`guid` (string): credential vault entry, resolved via `CQ.Credentials.getByGUID`.	`this`
`CreateTicket(fields)`	See below.	`IntegrationHTTPResponse`

`CreateTicket({summary, description, priority, extra_fields})` creates a ticket in the `incident` table. `extra_fields` accepts `urgency`, `impact`, `category`, and `assigned_to`; all are optional and omitted from the request when not set.

ConnectWise

Method	Parameters	Returns
`setHost(value)`	`value` (string): ConnectWise instance base URL.	`this`
`getHost()`	None.	Configured host string. Throws if no host is set.
`setBasicAuth(username, password)`	Basic-auth strings; ConnectWise expects `username` already formatted as `{companyId}+{publicKey}` and `password` as the private key.	`this`
`setCredentialsByGUID(guid)`	`guid` (string): credential vault entry.	`this`
`setClientId(id)`	`id` (string): ConnectWise `clientId` header.	`this`
`CreateTicket(fields)`	See below.	`IntegrationHTTPResponse`

`CreateTicket({summary, description, priority, extra_fields})` creates a service ticket. `extra_fields.company_id` and `extra_fields.company_name` are **required** — the call fails locally (no HTTP request is made) if either is missing. `extra_fields.board_id` / `extra_fields.board_name` are optional.

Remedy

Method	Parameters	Returns
`setHost(value)`	`value` (string): Remedy/Helix ITSM base URL.	`this`
`getHost()`	None.	Configured host string. Throws if no host is set.
`setBasicAuth(username, password)`	Username/password used to obtain an AR-JWT session token.	`this`
`setCredentialsByGUID(guid)`	`guid` (string): credential vault entry.	`this`
`CreateTicket(fields)`	See below.	`IntegrationHTTPResponse`

`CreateTicket({summary, description, priority, extra_fields})` logs in automatically on first use (form-encoded, obtaining an AR-JWT token that is reused for subsequent calls) and creates an incident. `extra_fields` accepts `urgency`, `impact`, `first_name`, `last_name`, `assigned_group`, and `status`.

Automatic Lookback on Events

CYBERQUEST Data Transformation Service (DTS) scripts can search previously received events. This lets you correlate new information, such as an Indicator of Compromise (IOC), with historical activity and create an alert when matching events are found.

Create alerts

The global `Alert` object provides two methods for creating alerts.

`Alert.create(options): void`

Creates an alert from an options object:

```
/** @type {Record<string, unknown>} */
const eventObject = {
    EventID: 100000,
    LocalTime: moment().format("YYYY-MM-DD HH:mm:ss.SSS")
};

Alert.create({
    template: "template name",
    logs: [eventObject],
    name: "alert name",
    emails: "analyst@example.com, soc@example.com",
    description: "alert description",
    secLevel: 8,
    secScore: 80,
    metaData: "additional metadata"
});
```

`options` is required and must be a non-null object. Its properties are optional:

Property	Type	Required	Default and behavior
`template`	`string`	No	Alert template name. Defaults to `""`.
`logs`	`Array<object>`	No	Event objects to associate with the alert. Defaults to an empty array. A non-array value is also treated as an empty array.
`name`	`string`	No	Alert name. Defaults to `"NewAlert"` when omitted or when its length is less than three characters.
`emails`	`string | Array<string>`	No	A comma-separated string or an array of email addresses. Defaults to no recipients. Invalid addresses are discarded.
`description`	`string`	No	Alert description. Defaults to `"NewAlert description"` when omitted or when its length is less than three characters.
`secLevel`	`number`	No	A finite security level from `0` through `10`, inclusive. Defaults to `0` when omitted, out of range, or not a finite number.
`secScore`	`number`	No	A finite security score from `0` through `100`, inclusive. Defaults to `0` when omitted, out of range, or not a finite number.
`metaData`	`unknown`	No	Additional alert metadata. Defaults to `""`.

Strings containing email addresses are split on commas. Leading and trailing whitespace is removed from each valid address.

Returns: `void`.

`Alert.createSimple(alert): void`

Sends a serialized alert payload directly:

```
/** @type {Record<string, unknown>} */
const eventObject = {
    EventID: 100000,
    LocalTime: moment().format("YYYY-MM-DD HH:mm:ss.SSS")
};

Alert.createSimple(JSON.stringify({
    logs: [eventObject],
    GeneratedTime: moment().format("YYYY-MM-DD HH:mm:ss.SSS"),
    IsAlert: "1",
    AlertSecurityLevel: 9,
    AlertSecurityScore: 90,
    AlertName: "IOC found in historical events",
    TemplateName: "",
    Description: "A known IOC matched historical activity.",
    Why: "The source or destination IP matched the IOC.",
    Category: "Security",
    SubCategory: "Threat intelligence",
    Tenant: "Tenant-name",
    MitreID: "T1071"
}));
```

The `alert` parameter is required and has type `string`. It must contain the complete serialized alert payload expected by the receiving service. `Alert.createSimple` forwards the string unchanged; it does not parse or validate it. The example payload uses the following fields:

Field	Type	Required
`logs`	`Array<object>`	Depends on the receiving service
`GeneratedTime`	`string`	Depends on the receiving service
`IsAlert`	`string`	Depends on the receiving service
`AlertSecurityLevel`	`number`	Depends on the receiving service
`AlertSecurityScore`	`number`	Depends on the receiving service
`AlertName`	`string`	Depends on the receiving service
`TemplateName`	`string`	Depends on the receiving service
`Description`	`string`	Depends on the receiving service
`Why`	`string`	Depends on the receiving service
`Category`	`string`	Depends on the receiving service
`SubCategory`	`string`	Depends on the receiving service
`Tenant`	`string`	Depends on the receiving service
`MitreID`	`string`	Depends on the receiving service

These fields illustrate the payload used by this example; the local API does not define their requiredness or default values.

Returns: `void`.

Use `Alert.create` for the standard options-based API. Use `Alert.createSimple` only when you already have the complete serialized alert payload required by the receiving service.

Search historical events

The global `Events` object provides the following lookback methods:

```
Events.getCount(query, days = 0); // number | false
Events.getBackLogs(query, days = 0, count = 100); // Array<object> | false
```

`Events.getCount(query, days = 0): number | false`

Parameter	Type	Required	Description
`query`	`string`	Yes	Elasticsearch query-string expression used to match events.
`days`	`number`	No	Finite number of days to look back. Defaults to `0`.

Returns: `number` containing the number of matching events, or `false` when `days` is not a finite number. Unlike `getBackLogs`, this method does not explicitly reject a negative `days` value.

`Events.getBackLogs(query, days = 0, count = 100): Array<object> | false`

Parameter	Type	Required	Description
`query`	`string`	Yes	Elasticsearch query-string expression used to match events. It must contain at least two characters.
`days`	`number`	No	Finite, non-negative number of days to look back. Defaults to `0`.
`count`	`number`	No	Finite maximum number of events to return. Defaults to `100`.

Returns: `Array<object>` containing up to `count` matching events, ordered by `LocalTime` in descending order (newest first). Returns `false` when the query is too short, either numeric argument is not a finite number, or `days` is negative.

Example: correlate an IOC with historical events

In **Rules** > **DTS Objects**, add an object and create a custom script. The following example searches the previous 30 days for events involving either of two IP addresses. It creates an alert when more than two events match:

```
const query = "SrcIP:192.168.1.1 OR DestIP:192.168.0.1";
const numberOfEvents = Events.getCount(query, 30);

if (numberOfEvents > 2) {
    const matchingEvents = Events.getBackLogs(query, 30, 100);

    Alert.create({
        emails: "analyst@example.com, soc@example.com",
        logs: matchingEvents,
        name: "IOC found in historical events",
        description: "Known malicious IP addresses matched historical events.",
        secLevel: 5,
        secScore: 10,
        metaData: "Matched by a DTS threat-intelligence lookback."
    });
}
```

For instructions on configuring the DTS object, see Create a DTS alert.

Support

Frequently Asked Questions

1. Why CYBERQUEST?

CYBERQUEST is a sophisticated platform that sits on top of all security-related data/applications/sensors/servers, Defined as a Security-Driven Analytics platform or "Next Generation SIEM". It gathers valuable data from multiple technology sources and empowers users to take actionable, critical decisions in real-time to keep the company safety.

Main benefits of the solution:

- suitable for SMBs as well as Enterprise
- predictable & no hidden costs – lowering the TCO
- unlimited flexibility for log/application data
- no vendor lock, NoSQL Database
- End-to-End Fast Deployment
- GDPR Compliance – fit per industry standards
- single point of access to all data
- reduces investigation time up to 10 times

2. How CYBERQUEST is licensed?

CYBERQUEST solution is available with Subscription or Perpetual for On-premise.

The licensing is based on CPU Cores.

The commercial editions are: **Logger, Light**, **Advanced**, **Enterprise** and **Ultimate**.

To check more detailed information please follow the link: CYBERQUEST Licensing and Versioning

3. What are the system requirements for CYBERQUEST?

CYBERQUEST is a virtual appliance but can be installed as a physical appliance as well.

To check detailed system requirements please follow the link: Minimum system requirements

4. How could I download the demo version of CYBERQUEST?

You can download the latest release demo version for Nextgen Software product on **https://nextgensoftware.eu/ (https://nextgensoftware.eu/)**.

5. How can I contact CYBERQUEST support team?

Service requests can be accessed through **https://portal.cyberquest.cloud/ (https://portal.cyberquest.cloud/)** or by email at support@nextgensoftware.eu.

6. What is a Log Records Structure for CYBERQUEST?

CYBERQUEST events can have the follwing fields:

Category	Field	Type	Description
Generic Fields			
	Category	string	Defines the classification of the event
	Computer	string	Hostname of the system that generated the event
	Description	string	Textual description or message associated with the event
	DestIP	string	IP address of the destination involved in the event
	DestIP_Country_Code	string	ISO country code for the destination IP
	DestIP_Country_Name	string	Country name associated with the destination IP
	DestMAC	string	MAC address of the destination device
	EventID	long	Unique identifier assigned to the event
	EventLog	string	Log where the event was recorded log
	EventPath	string	File system path related to the event (e.g., location of the affected file or process)
	EventType	long	Specifies the type of event that occurred
	GMT	date	Timestamp of the event in Coordinated Universal Time (UTC)
	ID	string	General identifier associated with the record
	IsIncident	boolean	If the event is categorized as security incident
	LocalTime	date	Local timestamp of the event occurrence
	N1 ... N40	long	general purpose numeric fields
	PlatformID	string	Identifier of the machine where the event originated
	PostDtsSHA256	string	log hash after passing through Data Transformation Service
	PreDtsSHA256	string	log hash before passing through Data Transformation Service
	RawData	string	raw data
	ReceivedTime	date	Time when the event was received or processed
	S1 ... S150	string	general purpose string fields
	SecondaryTag	string	secondary tag
	SessionID	string	Identifier for the session during which the event occurred
	Source	string	Origin or component related to the event
	SrcIP	string	IP address of the source involved in the event
	SrcIP_Country_Code	string	ISO country code for the source IP
	SrcIP_Country_Name	string	Country name associated with the source IP
	SrcMAC	string	MAC address of the source device
	Tag	string	Tag assigned to categorize the event
	isLastDuplicate		Boolean indicating if this is the most recent duplicate in a series
	Tenant	string	tenant
	TimeOfDay	long	time of day
	UserDomain	string	user domain
	UserName	string	username
	VersionMajor	long	version major

Category	Field	Type	Description
	VersionMinor	long	version minor
	content	string	content
	SecurityLevel	long	Numeric severity level assigned to the event, used to classify and prioritize events according to their security relevance
	SecurityScore	long	Numeric score indicating the security impact of the event, used for severity assessment and prioritization
	RiskAssessment	long	Numeric value representing the risk associated with the event, used to support risk-based analysis and prioritization
_Timestamp	SkewedOffset	long	the difference between real time and machine time
	Time	long	it is the number of seconds … as a scalar real number which represents the number of seconds that have passed since 00:00:00 UTC Thursday, 1 January 1970
	TimeZoneOffSet	long	adding the 80 seconds to the GMT
	isDST	boolean	the summer time if applied or not
_agent	GUID	string	Unique identifier for the agent
	Name	string	Name of the agent
	Site	string	Location or site associated with the relevant agent
_asset	Application	string	Application name associated with the asset
	Criticality	long	Criticality level of the asset (rating)
	Location		Physical or logical location of the asset
	Name	string	Name of the asset
	Owner	string	Owner of the asset
	Project	string	Associated project for the asset
	SecurityValue	long	Security rating or value of the asset
	Site	string	Asset site or location (city)
_attack	DestIP	string	destination IP is the IP address of the device to which the packet is being sent.
	GeoCity	string	decoded City from IP address
	GeoCountry	string	decoded Country from IP address
	Host	string	is a computer or other device that communicates with other hosts on a network, include clients and servers – that send or receive data, services or applications
	GeoLat	GEO	decoded latitude from IP address
	GeoLong	GEO	decoded longitude from IP address
	Method	string	is a particular procedure for accomplishing or approaching something, especially a systematic or established one.
	Object	string	network objects are used to categorize IP addresses into different types of network entities
	OtherInfo	String	other information about our network
	Result	boolean	the result of the attack

Category	Field	Type	Description
	SrcIP	string	source IP is the IP (Internet Protocol) address of the device sending the IP packet (the IP unit of data transfer).
	TriggeredRule	string	is use to define conditions under which a trigger action is to be executed.
_dataSource	Name	string	Name of the data source
	SecurityAppliance	string	Physical name of the data source
	Version	string	Version of the data source generating the event
_event	Category	string	Context-specific classification assigned to the event by CYBERQUEST
	Result	boolean	Indicates the outcome of the event (e.g., success or failure)
	SourceObject	string	Object within the system that originated the event, providing a more precise indication of its source
	SourceUser	string	User who triggered or is associated with the event, providing a more precise indication of their origin
	SubCategory	string	Subcategory classification assigned by CYBERQUEST based on the event's main category
	TargetObject	string	Object targeted by the event, indicating a more precise destination or endpoint
	TargetUser	string	User targeted by the event, representing the intended recipient or destination of the action
	URL	string	URL associated with the event, identifying the location of a resource involved in the activity
	CorrelationID		ID used to correlate related events
_forensics	What	string	Action or activity that occurred
	Where	string	Location where the event or incident took place
	Who	string	Individual or entity responsible for or involved in generating the event
	Why	string	Reason the event was generated
_geoLocation	DestIPGeoCountry	string	Destination IP coordinates of the country
	DestIPGeoPoint	geo_point	Geolocation point of the destination IP
	DestIPGeocity	string	Destination IP coordinates of the city
	Host	string	Hostname associated with geolocation context
	SrcIPGeoCountry	string	Source IP coordinates of the country
	SrcIPGeoPoint	geo_point	Geolocation point of the source IP
	SrcIPGeocity	string	Source IP coordinates of the city
_incident	Category	string	Classification of the incident assigned by CYBERQUEST
	Impact	string	Impact assessment of the incident, measuring the extent and potential damage before resolution
	Score	long	Score assigned to quantify the severity of an unplanned situation that disrupts or degrades an IT service
	SubCategory	string	Subclassification of the incident assigned by CYBERQUEST based on its main category
_malware	DeliveryMethod	string	deliveryMethod (mail, file etc…)

Category	Field	Type	Description
	Name	string	Name of the malware identified
_network	AplicationName	string	Application name involved in the network event
	DestIPv4	ip	Destination IPv4 address in the network context
	DestIPv6	string	Destination IPv6 address in the network context
	DestInterface	string	Network interface used by the destination
	DestPort	long	Destination port used in the network connection
	FlowID	string	Identifier of the network flow
	PostNATDestIPv4	ip	Dest IPv4 address after NAT translation
	PostNATDestIPv6	string	Dest IPv6 address after NAT translation
	PostNATDestPort	long	Destination port after NAT translation
	PostNATSrcIPv4	ip	Source IPv4 address after NAT translation
	PostNATSrcIPv6	string	Source IPv6 address after NAT translation
	PostNATSrcPort	long	Source port after NAT translation
	Protocol	string	Network protocol used (e.g., TCP, UDP)
	ReceivedBytes	long	Number of bytes received through the network
	SrcIPv4	ip	Source IPv4 address in the network context
	SrcIPv6	string	Source IPv6 address in the network context
	SrcInterface	string	Interface used by the source in the network
	SrcPort	long	Source port used in the network connection
	ClientIPGeoCity		City location of the client IP
	ClientIP		Client IP address in the network
	TransferedBytes	long	Total bytes transferred in the network flow
_risk	RiskScoreAsset		Risk score assigned to the affected asset
	RiskScoreUser		Risk score assigned to the affected user
	RiskNames		Named risks identified for the event
	FullRuleMatch		Details of full rule matches that triggered the risk
	RiskScoreEvent		Risk score associated with the event
	GeoCountry		Country location associated with the attack context
	DestIP		Destination IP involved in the attack context
	TriggeredRule		Security rule that was triggered by the attack
	Host		Host targeted in the attack
	Object		Object targeted or affected during the attack
	Method		Method or technique used in the attack
	GeoCity		City location associated with the attack context
	SrcIP		Source IP used in the attack
	Location		Location context of the attack
	OtherInfo		Additional context or metadata for the attack
	Result		Result or outcome of the attack

7. Alert Records Structure

CYBERQUEST Alerts can have the follwing fields:

Category	Field	Type	Description
Generic Fields			
	Category	string	Classification or type assigned to the event
	Computer	string	Name of the computer where the event was generated
	Description	string	Textual description or message associated with the event
	DestIP	string	IP address of the destination involved in the event
	EventID	long	Unique identifier assigned to the event
	EventLog	string	Log where the event was recorded log
	EventType	long	Specifies the type of event that occurred
	GMT	date	Timestamp of the event in Coordinated Universal Time (UTC)
	LocalTime	date	Local timestamp of the event occurrence
	PlatformID	string	Identifier of the machine where the event originated
	S1...S150	string	General purpose string fields
	Destination Port	long	Destination port
	Application name	string	Application name
	SourcePort	string	source port
	Flow ID	string	NetflowID
	Source	string	source
	SrcIP	string	source IP is the IP (Internet Protocol) address of the device sending the IP packet (the IP unit of data transfer)
	Tag	string	tag
	VersionMajor	long	version major
	VersionMinor	long	version minor
	ReceivedTime	date	received time
	SecurityScore	long	Numeric score indicating security impact of the event
	SecurityLevel	long	security level
	SrcIP_Country_Code	string	country code of SrcIP
	SrcIP_Country_Name	string	country name of SrcIP
	DestIP_Country_Code	string	country code of DestIP
	DestIP_Country_Name	string	country name of DestIP
	EventPath	string	event path
	TimeOfDay	long	time of day
_anomaly	AnomalyID		Identifier of the anomaly detected
	RelativeScore		Relative score representing anomaly severity
	Score		Absolute score of the anomaly detected
_network	AplicationName	string	application name
	DestIPv4	ip	destination IP(IPv4)
	DestInterface	string	destination interface
	DestPort	long	destination port

Category	Field	Type	Description
	FlowID	string	NetflowID
	PostNATDestIPv4	ip	destination IP(IPv4) after network translation
	PostNATDestPort	long	destination port after network translation
	PostNATSrcIPv4	ip	source IP(IPv4) after network translation
	PostNATSrcPort	long	source port after network translation
	Protocol	string	protocol
	ReceivedBytes	long	received bytes
	SrcIPv4	ip	destination IP(IPv4)
	SrcInterface	string	source interface
	SrcPort	long	source port
	TransferedBytes	long	transferred bytes
_Timestamp	isDST	boolean	Indicates whether the timestamp falls within Daylight Saving Time (summer time) period
	TimeZoneOffSet	long	Time zone offset applied to the timestamp, representing the difference from GMT/UTC
	SkewedOffset	long	Offset representing the difference between the system's time and the actual (real) time
	Time	long	Recorded event time represented as the number of seconds elapsed since 00:00:00 UTC on January 1, 1970 (Unix epoch time)
_asset	GUID	string	asset globally unique identifier
	Name	string	the actual name of asset
	SecurityValue	long	security level
_event	Category	string	a category is assigned by CYBERQUEST for each event
	SubCategory	string	a Subcategory is assigned by CYBERQUEST for each event depending on the main category
_geoLocation	SrcIPGeoCountry	string	source IP coordinates of the country
	SrcIPGeocity	string	source IP coordinates of the city
	SrcIPGeoPoint	geo_point	source IP coordinates of the point
	DestIPGeoCountry	string	destination IP coordinates of the country
	DestIPGeocity	string	destination IP coordinates of the city
	DestIPGeoPoint	geo_point	destination IP coordinates of the point

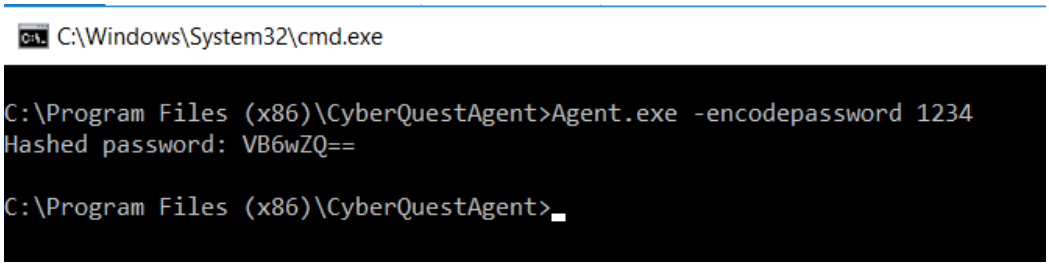
Additional utilities

How to encode a password for collecting events from domain computers

The password is encoded on a station where the CYBERUQEST Agent is installed. To encode the password, follow these steps:

1. Open a CMD window;
2. Navigate to **"C:\Program Files (x86)\CyberQuestAgent"**, where the CYBERQUEST Agent is installed.
3. Execute command **"Agent.exe -encodepassword=1234**, where "1234" is the password that should be encoded.

4. The result is a hashed password, as shown below:



Troubleshooting

Web Interface Errors and Probable Issues

1. The error occurs in the web interface/Case 1

Error: An Internal Error Has Occurred. Please check that the required services are running.

Probably the mysql server is off/crash. Check mysql server using ssh with the following command:

```
systemctl status mysql.service
```

If the service does not look like it's running:

```
mysql.service - LSB: Start and stop the mysql database server daemon
 Loaded: loaded (/etc/init.d/mysql)
 Active: inactive (dead) since Mon 2016-09-12 09:37:28 EEST; 1min 43s ago
 Process: 15510 ExecStop=/etc/init.d/mysql stop (code=exited, status=0/SUCCESS)
 Process: 548 ExecStart=/etc/init.d/mysql start (code=exited, status=0/SUCCESS)
```

The problem is resolved with the **mysql.service restart** system, using the following command:

```
systemctl restart mysql.service
```

Check using the following command:

```
systemctl status mysql.service
```

The result should look like this:

```
mysql.service - LSB: Start and stop the mysql database server daemon
   Loaded: loaded (/etc/init.d/mysql)
   Active: active (running) since Mon 2016-09-12 09:40:48 EEST; 2s ago
  Process: 15510 ExecStop=/etc/init.d/mysql stop (code=exited, status=0/SUCCESS)
  Process: 15959 ExecStart=/etc/init.d/mysql start (code=exited, status=0/SUCCESS)
```

2. The error occurs in the web interface/Case 2

Error: Connecting to the main datastore. Are all the services running? Connection refused

Probably the mysql server is off/crash. Check mysql server using ssh with the following command:

```
systemctl status mysql.service
```

If the service does not look like it's running :

```
mysql.service - LSB: Start and stop the mysql database server daemon
   Loaded: loaded (/etc/init.d/mysql)
   Active: inactive (dead) since Mon 2016-09-12 09:37:28 EEST; 1min 43s ago
  Process: 15510 ExecStop=/etc/init.d/mysql stop (code=exited, status=0/SUCCESS)
  Process: 548 ExecStart=/etc/init.d/mysql start (code=exited, status=0/SUCCESS)
```

The problem is resolved with the **mysql.service restart** system, using the following command:

```
systemctl restart mysql.service
```

Check using the following command:

```
systemctl status mysql.service
```

The result should look like this:

```
mysql.service - LSB: Start and stop the mysql database server daemon
   Loaded: loaded (/etc/init.d/mysql)
   Active: active (running) since Mon 2016-09-12 09:40:48 EEST; 2s ago
  Process: 15510 ExecStop=/etc/init.d/mysql stop (code=exited, status=0/SUCCESS)
  Process: 15959 ExecStart=/etc/init.d/mysql start (code=exited, status=0/SUCCES
```

Or probably Online DataStorage is off/crash. Check Online DataStorage service using ssh with the following command:

```
systemctl status opensearch.service
```

If the service does not look like it's running :

```
opensearch.service - opensearch init script wrapper
     Loaded: loaded (/lib/systemd/system/opensearch.service; enabled; vendor preset: enabled)
     Active: failed (Result: exit-code) since Fri 2023-04-28 13:13:38 EEST; 2 min 5s ago
    Process: 3416812 ExecStart=/bin/bash -c /usr/bin/docker compose -f /var/opt/cyberquest/compose/docker-compose.yml
up opensearch > /var/log/opensearch.log (code=exited, status=1/FAILURE)
   Main PID: 3416812 (code=exited, status=1/FAILURE)
        CPU: 124ms
```

The problem is resolved with the ** opensearch.service restart** system, using the following command:

```
systemctl restart opensearch.service
```

Check using the following command:

```
systemctl status opensearch.service
```

The result should look like this:

```
opensearch.service - opensearch init script wrapper
     Loaded: loaded (/lib/systemd/system/opensearch.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2023-05-08 14:58:30 EEST; 23s ago
   Main PID: 52055 (bash)
      Tasks: 19 (limit: 19172)
     Memory: 22.7M
        CPU: 141ms
     CGroup: /system.slice/opensearch.service
             ├─52055 /bin/bash -c /usr/bin/docker compose -f /var/opt/cyberquest/compose/docker-compose.yml up opense
arch > /var/log/opensearch.log
             ├─52056 /usr/bin/docker compose -f /var/opt/cyberquest/compose/docker-compose.yml up opensearch
             └─52070 /usr/libexec/docker/cli-plugins/docker-compose compose -f /var/opt/cyberquest/compose/docker-com
pose.yml up opensearch
```

3. The error occurs in the web interface/Case 3

Error: Connecting to the main datastore. Are all the services running? Online DataStorage Error: Error

Probably Online DataStorage is off/crash. Check Online DataStorage service using ssh with the following command:

```
systemctl status opensearch.service
```

If the service does not look like it's running:

```
opensearch.service - opensearch init script wrapper
     Loaded: loaded (/lib/systemd/system/opensearch.service; enabled; vendor preset: enabled)
     Active: failed (Result: exit-code) since Fri 2023-04-28 13:13:38 EEST; 2 min 5s ago
    Process: 3416812 ExecStart=/bin/bash -c /usr/bin/docker compose -f /var/opt/cyberquest/compose/docker-compose.yml
up opensearch > /var/log/opensearch.log (code=exited, status=1/FAILURE)
   Main PID: 3416812 (code=exited, status=1/FAILURE)
        CPU: 124ms
```

The problem is resolved with the ** opensearch.service restart** system, using the following command:

```
systemctl restart opensearch.service
```

Check using the following command:

```
systemctl status opensearch.service
```

The result should look like this:

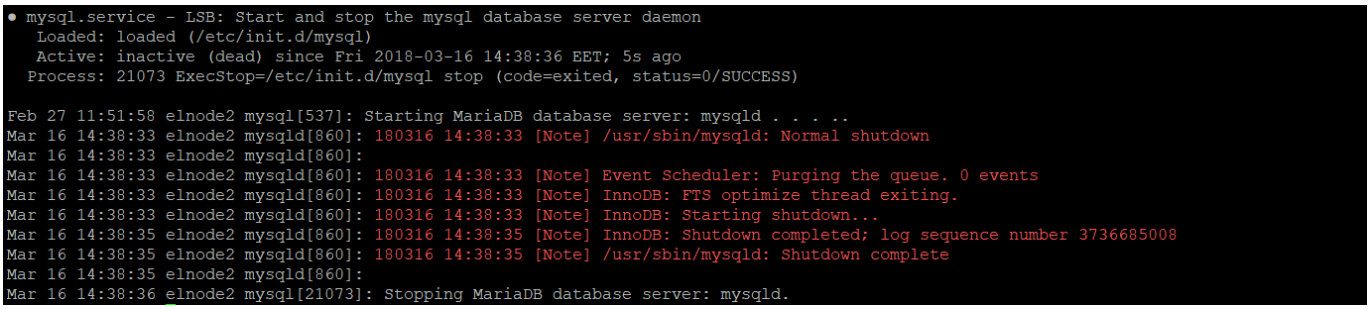
```
opensearch.service - opensearch init script wrapper
     Loaded: loaded (/lib/systemd/system/opensearch.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2023-05-08 14:58:30 EEST; 23s ago
   Main PID: 52055 (bash)
      Tasks: 19 (limit: 19172)
     Memory: 22.7M
        CPU: 141ms
     CGroup: /system.slice/opensearch.service
             ├─52055 /bin/bash -c /usr/bin/docker compose -f /var/opt/cyberquest/compose/docker-compose.yml up opense
arch > /var/log/opensearch.log
             ├─52056 /usr/bin/docker compose -f /var/opt/cyberquest/compose/docker-compose.yml up opensearch
             └─52070 /usr/libexec/docker/cli-plugins/docker-compose compose -f /var/opt/cyberquest/compose/docker-com
pose.yml up opensearch
```

4. Mysql service off

The error which appears in the “putty” with the corresponding host name (or ip address) and the port and also the connection type (SSH) using the command:

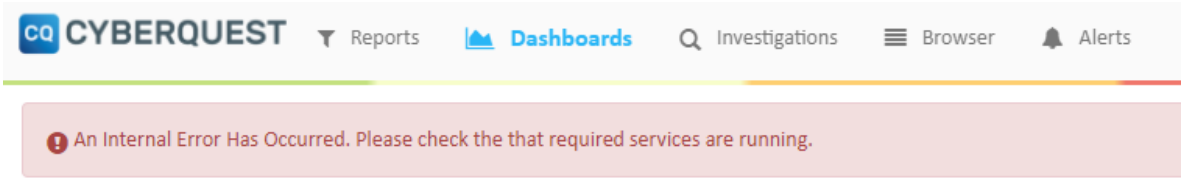
```
systemctl status mysql.service
```

And the error following commands:



Now if we go into the web application this will be the error that will occur:

Error: An Internal Error Has Occurred. Please check the that required services are running



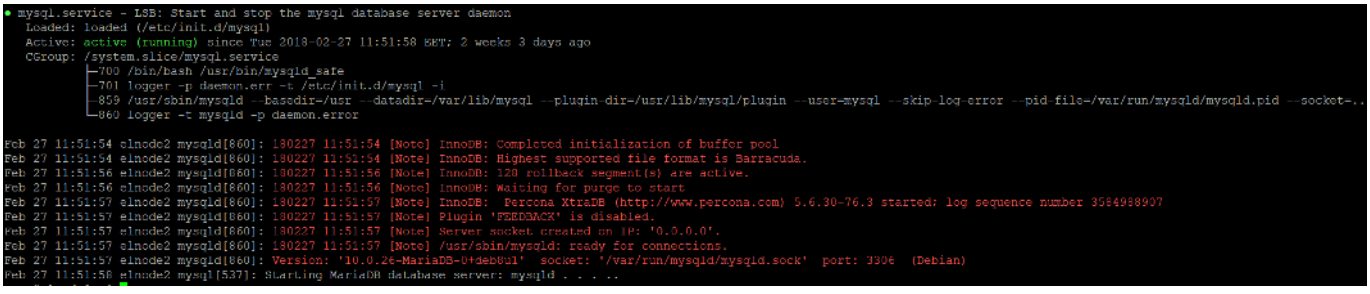
The resolving method is to restart mysql service by following the command:

```
systemctl restart mysql.service
```

Check using the following command:

```
systemctl status mysql.service
```

And the result of the command is the following:



5. Online DataStorage service off

The error which appears in the “putty” with the corresponding host name (or ip address) and the port and also the connection type (SSH) using the command:

```
systemctl status opensearch.service
```

And the error following commands:

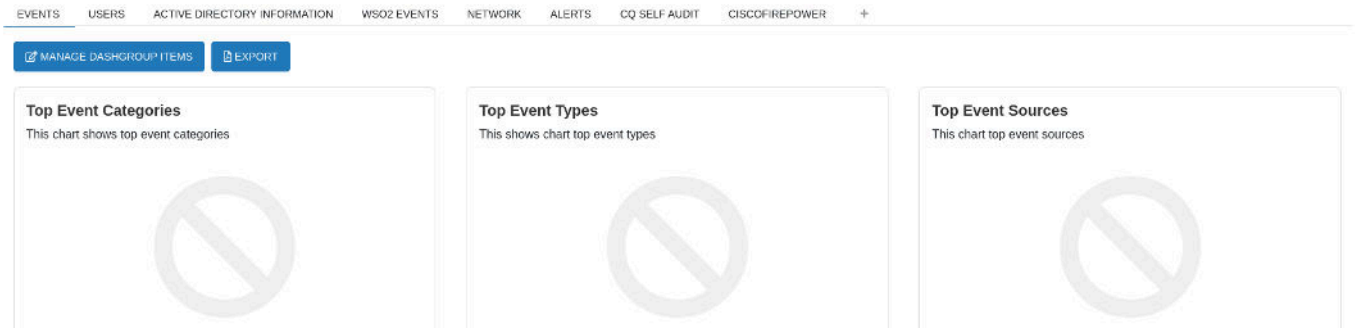
```
root@cyberquest:~# systemctl status opensearch.service
● opensearch.service - opensearch init script wrapper
     Loaded: loaded (/lib/systemd/system/opensearch.service; enabled; vendor preset: enabled)
     Active: failed (Result: exit-code) since Fri 2023-04-28 13:13:38 EEST; 1 weeks 3 days ago
    Process: 3416812 ExecStart=/bin/bash -c /usr/bin/docker compose -f /var/opt/cyberquest/compose/docker-compose.yml up opensearch > /var/log/opensearch.log (code=exited, status=1/FAILURE)
   Main PID: 3416812 (code=exited, status=1/FAILURE)
        CPU: 124ms

Warning: journal has been rotated since unit was started, output may be incomplete.
```

Now if we go into cerebro web plugin (**http://CyberquestIP:9000**) will show the following error:



Or if we go into the web application this will be the error that will occur and there is no data available:



The resolving method is to restart the service by following the command:

```
systemctl restart opensearch.service
```

Check using the following command:

```
systemctl status opensearch.service
```

And the result of the command is the following:

```
● opensearch.service - opensearch init script wrapper
     Loaded: loaded (/lib/systemd/system/opensearch.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2023-05-08 14:58:30 EEST; 23s ago
   Main PID: 52055 (bash)
      Tasks: 19 (limit: 19172)
     Memory: 22.7M
        CPU: 141ms
     CGroup: /system.slice/opensearch.service
             ├─52055 /bin/bash -c /usr/bin/docker compose -f /var/opt/cyberquest/compose/docker-compose.yml up opensearch > /var/log/opensearch.log
             ├─52056 /usr/bin/docker compose -f /var/opt/cyberquest/compose/docker-compose.yml up opensearch
             └─52070 /usr/libexec/docker/cli-plugins/docker-compose compose -f /var/opt/cyberquest/compose/docker-compose.yml up opensearch
```

6. Rabbitmq-server service stopped

The error which appears in the “putty” with the corresponding host name (or ip address) and the port and also the connection type (SSH) using the command:

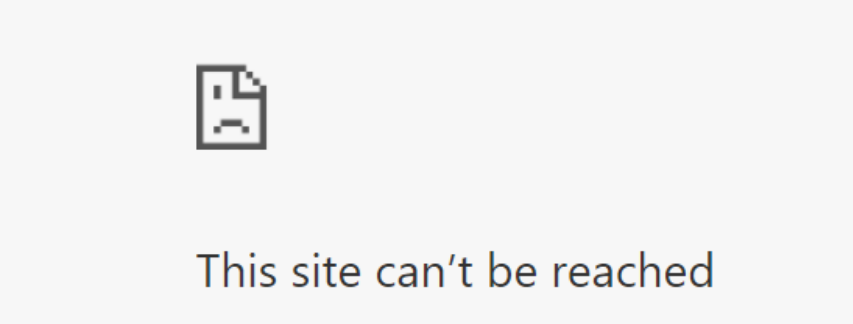
```
systemctl status rabbitmq-server.service
```

And the error following commands:

```
● rabbitmq-server.service - LSB: Enable AMQP service provided by RabbitMQ broker
   Loaded: loaded (/etc/init.d/rabbitmq-server)
   Active: inactive (dead) since Fri 2018-03-16 14:10:41 EET; 1min 23s ago
  Process: 14043 ExecStop=/etc/init.d/rabbitmq-server stop (code=exited, status=0/SUCCESS)

Feb 27 11:52:13 elnode2 rabbitmq-server[540]: Starting message broker: rabbitmq-server.
Mar 16 14:10:37 elnode2 su[14054]: Successful su for rabbitmq by root
Mar 16 14:10:37 elnode2 su[14054]: + ??? root:rabbitmq
Mar 16 14:10:37 elnode2 su[14054]: pam_unix(su:session): session opened for user rabbitmq by (uid=0)
Mar 16 14:10:38 elnode2 su[14054]: pam_unix(su:session): session closed for user rabbitmq
Mar 16 14:10:38 elnode2 su[14103]: Successful su for rabbitmq by root
Mar 16 14:10:38 elnode2 su[14103]: + ??? root:rabbitmq
Mar 16 14:10:38 elnode2 su[14103]: pam_unix(su:session): session opened for user rabbitmq by (uid=0)
Mar 16 14:10:41 elnode2 su[14103]: pam_unix(su:session): session closed for user rabbitmq
Mar 16 14:10:41 elnode2 rabbitmq-server[14043]: Stopping message broker: rabbitmq-server.
```

Now if we go into rabbitmq web plugin (**http://CyberquestIP:15672**) does not work:



The resolving method is to restart the service by following the commands:

```
systemctl restart rabbitmq-server.service
```

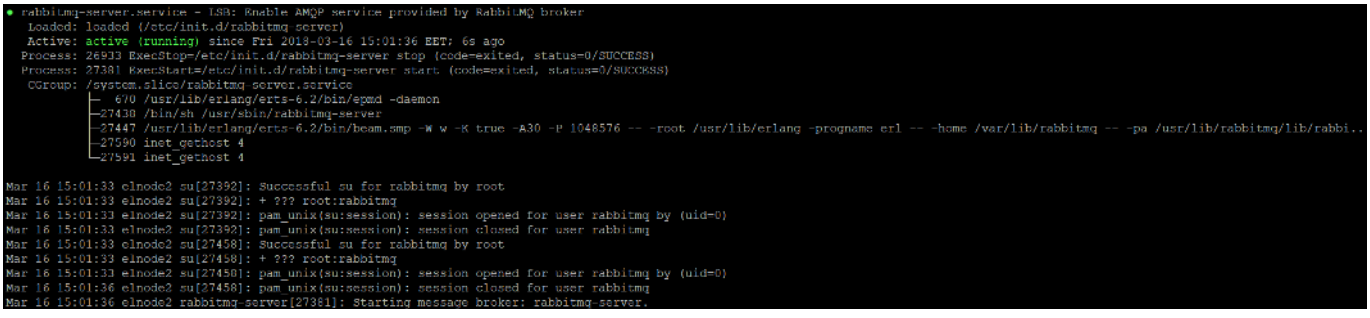
AND

```
systemctl restart data-acquisition.service
```

Check using the following command:

```
systemctl status rabbitmq-server.service
```

And the result of the command is the following:



7. Nginx.service service stopped

The error which appears in the "putty" with the corresponding host name (or ip address) and the port and also the connection type (SSH) using the command:

```
systemctl status nginx.service
```

And the error following commands:

```
● nginx.service - A high performance web server and a reverse proxy server
   Loaded: loaded (/lib/systemd/system/nginx.service; enabled)
   Active: inactive (dead) since Fri 2018-03-16 16:44:00 EET; 11s ago
  Process: 17846 ExecStop=/sbin/start-stop-daemon --quiet --stop --retry QUIT/5 --pidfile /run/nginx.pid (code=exited, status=0/SUCCESS)
 Main PID: 641 (code=exited, status=0/SUCCESS)
```

Or if we go into the web application this will be the error that will occur:



The resolving method is to restart the service by following the command:

```
systemctl restart nginx.service
```

Check using the following command:

```
systemctl status nginx.service
```

The result of the command is the following:

```
● nginx.service - A high performance web server and a reverse proxy server
   Loaded: loaded (/lib/systemd/system/nginx.service; enabled)
   Active: active (running) since Fri 2018-03-16 16:58:43 EET; 2s ago
  Process: 17846 ExecStop=/sbin/start-stop-daemon --quiet --stop --retry QUIT/5 --pidfile /run/nginx.pid (code=exited, status=0/SUCCESS)
  Process: 23629 ExecStart=/usr/sbin/nginx -g daemon on; master_process on; (code=exited, status=0/SUCCESS)
  Process: 23625 ExecStartPre=/usr/sbin/nginx -t -q -g daemon on; master_process on; (code=exited, status=0/SUCCESS)
 Main PID: 23630 (nginx)
   CGroup: /system.slice/nginx.service
           ├─23630 nginx: master process /usr/sbin/nginx -g daemon on; master_process on;
           ├─23631 nginx: worker process
           ├─23632 nginx: worker process
           ├─23633 nginx: worker process
           └─23634 nginx: worker process
```

8. Php8.1-fpm.service service stopped

The error which appears in the “putty” with the corresponding host name (or ip address) and the port and also the connection type (SSH) using the command:

```
systemctl status php8.1-fpm.service
```

And the error following commands:

```
php8.1-fpm.service - The PHP 8.1 FastCGI Process Manager
   Loaded: loaded (/lib/systemd/system/php8.1-fpm.service; enabled; vendor preset: enabled)
   Active: inactive (dead) since Mon 2023-05-08 15:18:48 EEST; 8s ago
     Docs: man:php-fpm8.1(8)
  Process: 32732 ExecStart=/usr/sbin/php-fpm8.1 --nodaemonize --fpm-config /etc/php/8.1/fpm/php-fpm.conf (code=exited, status=0/SUCCESS)
  Process: 54098 ExecStopPost=/usr/lib/php/php-fpm-socket-helper remove /run/php/php-fpm.sock /etc/php/8.1/fpm/pool.d/www.conf 81 (code=exited, status=0/SUCCESS)
 Main PID: 32732 (code=exited, status=0/SUCCESS)
   Status: "Processes active: 0, idle: 5, Requests: 1762, slow: 0, Traffic: 0.1req/sec"
      CPU: 3min 51.658s
```

Or if we go into the web application this will be the error that will occur:



The resolving method is to restart the service by following the command:

```
systemctl restart php8.1-fpm.service
```

Check using the following command:

```
systemctl status php8.1-fpm.service
```

The result of the command is the following:

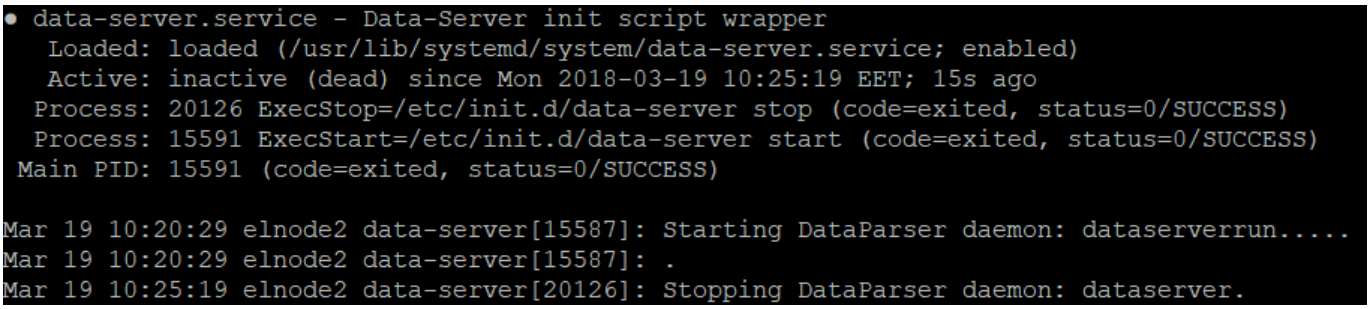


9. Data-storage.service service stopped

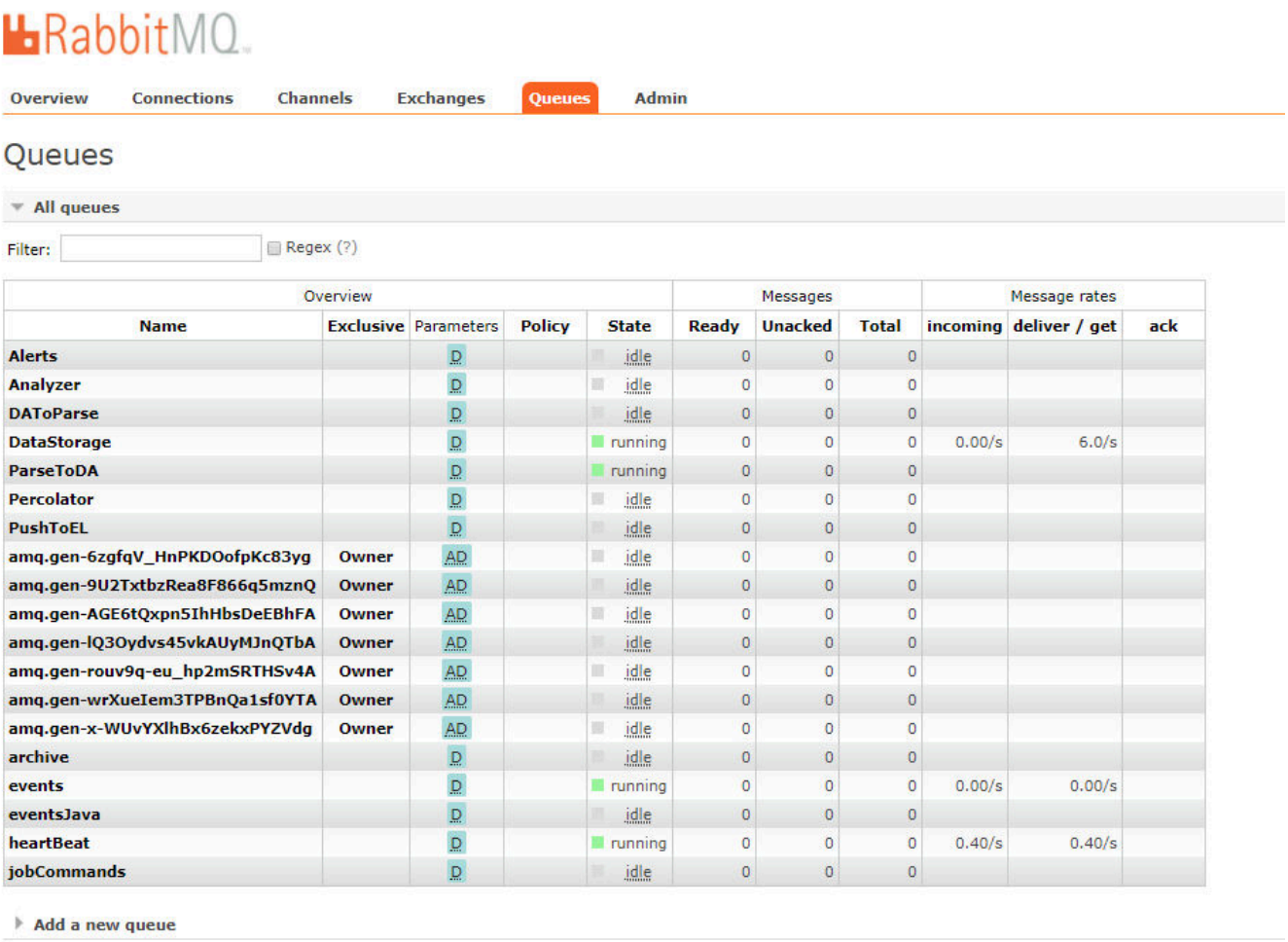
The error which appears in the “putty” with the corresponding host name (or ip address) and the port and also the connection type (SSH) using the command:

```
systemctl status data-storage.service
```

And the error following commands:



Events blocked on the queue in Data Storage on RabbitMQ(**http://CyberquestIP:15672**)



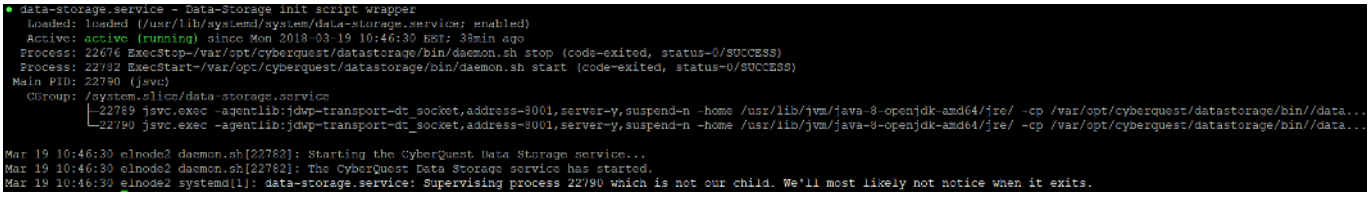
The resolving method is to restart the service by following the command:

```
systemctl restart data-storage.service
```

Check using the following command:

```
systemctl status data-storage.service
```

The result of the command is the following:



10. Data-acquisition.service service stopped

The error which appears in the “putty” with the corresponding host name (or ip address) and the port and also the connection type (SSH) using the command:

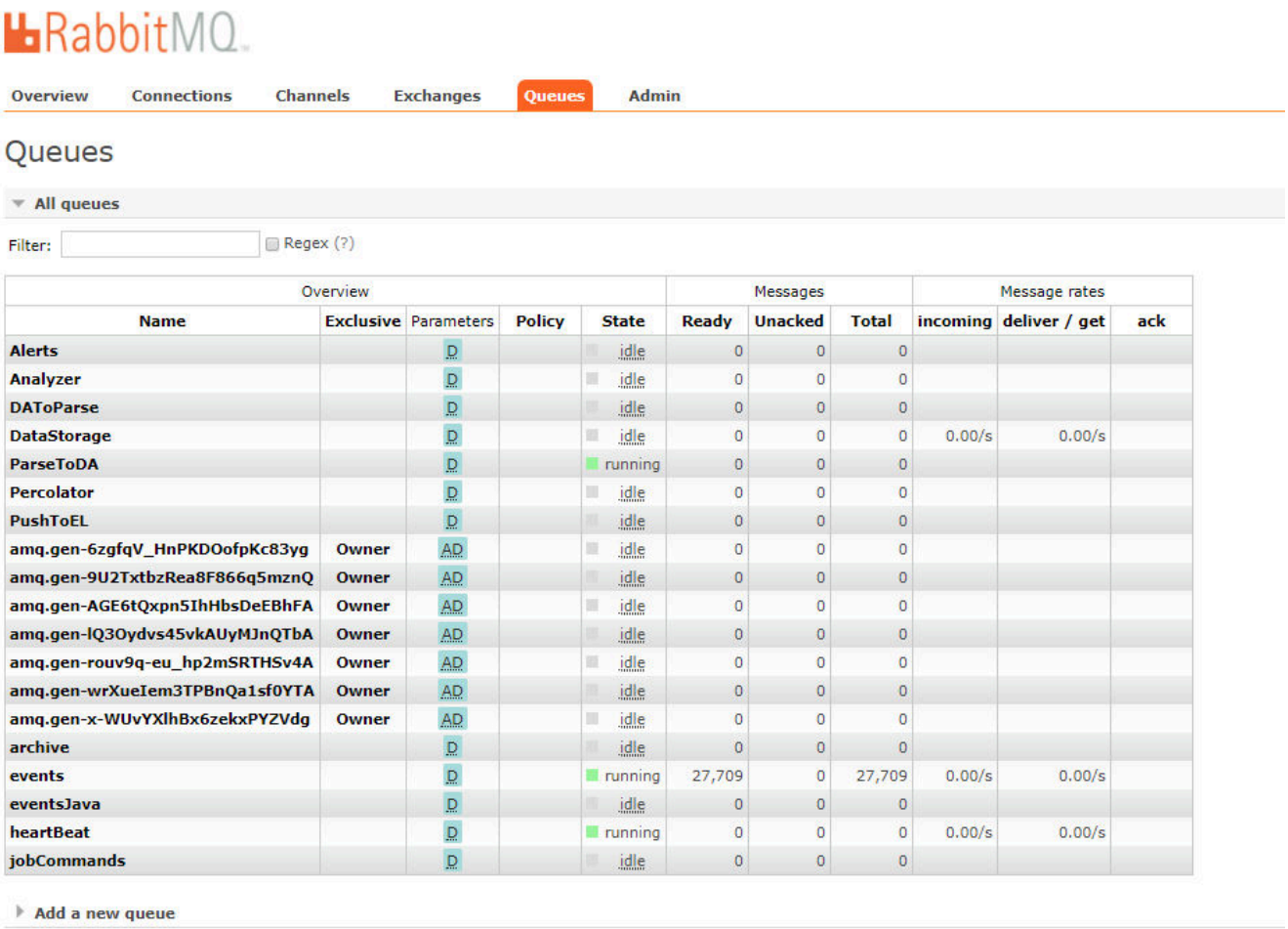
```
systemctl status data-acquisition.service
```

And the error following commands:

```
● data-acquisition.service - Data-Acquisition init script wrapper
   Loaded: loaded (/usr/lib/systemd/system/data-acquisition.service; enabled)
   Active: inactive (dead) since Mon 2018-03-19 11:31:59 EET; 6min ago
  Process: 2270 ExecStop=/etc/init.d/data-acquisition stop (code=exited, status=0/SUCCESS)
  Process: 3533 ExecStart=/etc/init.d/data-acquisition start (code=exited, status=0/SUCCESS)
 Main PID: 3533 (code=exited, status=0/SUCCESS)

Mar 16 15:40:15 elnode2 data-acquisition[3515]: Starting CyberQuest Data Acquisition daemon: dataacquisitions-a creat un comp event------------------------------
Mar 16 15:40:15 elnode2 data-acquisition[3515]: run.....
Mar 16 15:40:15 elnode2 data-acquisition[3515]: .
Mar 19 11:31:57 elnode2 data-acquisition[2270]: Stopping CyberQuest Data Acquisition daemon: dataacquisition failed!
```

Events blocked on the queue in data-acquisition.service on RabbitMQ (**http://CyberquestIP:15672**)



The resolving method is to restart the service by following the command:

```
systemctl restart data-acquisition.service
```

Check using the following command:

```
systemctl status data-acquisition.service
```

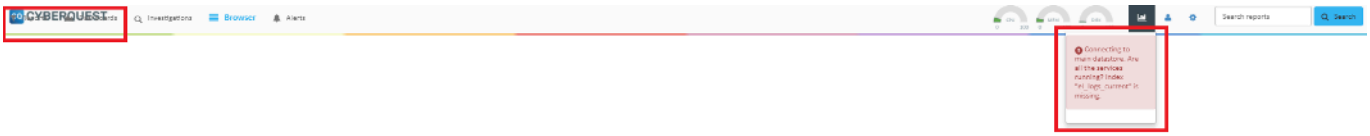
The result of the command is the following:

```
● data-acquisition.service - Data-Acquisition init script wrapper
   Loaded: loaded (/usr/lib/systemd/system/data-acquisition.service; enabled)
   Active: active (running) since Mon 2018-03-19 13:33:13 EET; 26s ago
  Process: 2270 ExecStop=/etc/init.d/data-acquisition stop (code=exited, status=0/SUCCESS)
 Main PID: 26536 (dataacquisition)
   CGroup: /system.slice/data-acquisition.service
           └─26536 /var/opt/cyberquest/dataacquisition/bin/dataacquisition /var/opt/cyberquest/dataacquisition/conf/config.ini

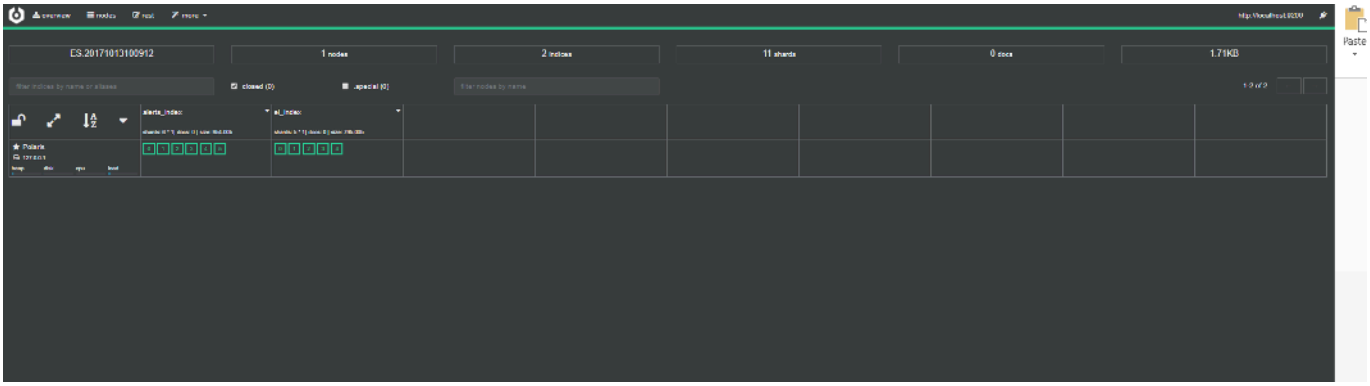
Mar 19 13:33:13 elnode2 data-acquisition[26518]: Starting CyberQuest Data Acquisition daemon: dataacquisitions-a creat un comp event------------------------------
Mar 19 13:33:13 elnode2 data-acquisition[26518]: run.....
Mar 19 13:33:13 elnode2 data-acquisition[26518]: .
```

Or if we go into the web application this will be the error that will occur:

ERROR: Connecting to the main datastore. Are all the services running? Index "el_logs_current" is missing



Now if we go into cerebro web plugin (**http://CyberquestIP:9000**) will show the following error:



The resolving method is to restart the service by following the command:

```
systemctl restart data-acquisition.service
```

11. Rsyslog service stopped (self-audit events)

The error which appears in the “putty” with the corresponding host name (or ip address) and the port and also the connection type (SSH) using the command:

```
/etc/init.d/rsyslog status
```

And the error following commands:

```
● rsyslog.service - System Logging Service
   Loaded: loaded (/lib/systemd/system/rsyslog.service; enabled)
   Active: inactive (dead) since Mon 2018-03-19 14:12:04 EET; 4s ago
     Docs: man:rsyslogd(8)
           http://www.rsyslog.com/doc/
 Main PID: 606 (code=exited, status=0/SUCCESS)
```

The resolving method is to restart the service by following the command:

```
/etc/init.d/rsyslog restart
```

And the result of the command is the following:

```
/etc/init.d/rsyslog status
```

```
● rsyslog.service - System Logging Service
   Loaded: loaded (/lib/systemd/system/rsyslog.service; enabled)
   Active: active (running) since Mon 2018-03-19 14:16:21 EET; 5s ago
     Docs: man:rsyslogd(8)
           http://www.rsyslog.com/doc/
 Main PID: 3658 (rsyslogd)
   CGroup: /system.slice/rsyslog.service
           └─3658 /usr/sbin/rsyslogd -n
```

Or another problem can be found in rsyslog.conf file:

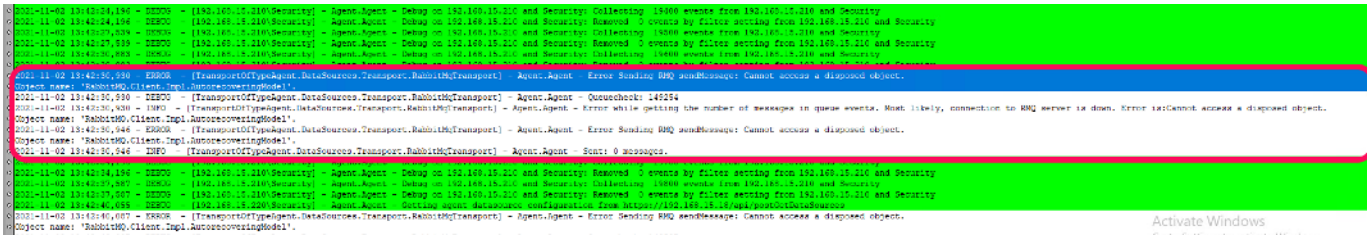
```
nano /etc/rsyslog.conf
```

Scroll down until you reach the end of the file and check if it matches the desired ip **(" *. * " - this symbol represents all types of events)**

```
daemon.*;mail.*;\
        news.err;\
        *.=debug;*.=info;\
        *.=notice;*.=warn       |/dev/xconsole
*.* @127.0.0.1:5140
#*.* @@192.168.115.115:8533
```

12. RabbitMQ error

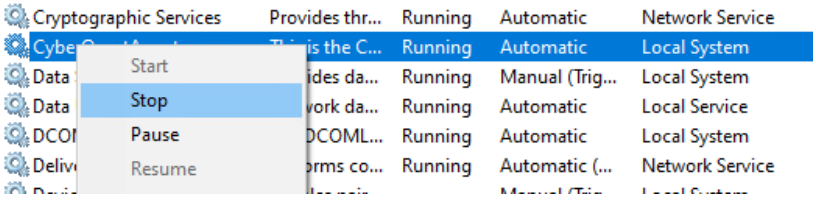
When this error occurs, we don't find new information in the web application. We find this error in CYBERQUEST logs. Using the baretail program we open the file(agent.txt) and we can view the error log.



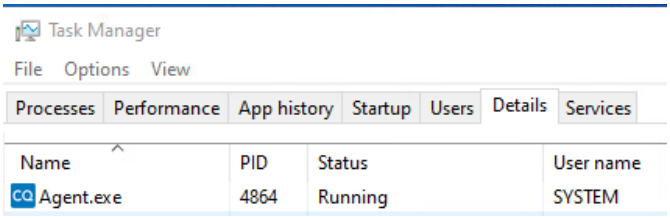
To solve the problem we have to stop the CYBERQUEST Agent and restart the RabbitMQ service. Follow the instructions for more details:

A. **Stop CYBERQUEST Agent**

On the Windows machine where the CYBERQUEST Agent is installed, open Windows Services and stop the CYBERQUEST Agent service.



To check if the CYBERQUEST Agent has stopped, open Task Manager > Details and wait until the Agent .exe process disappears from Task Manager.



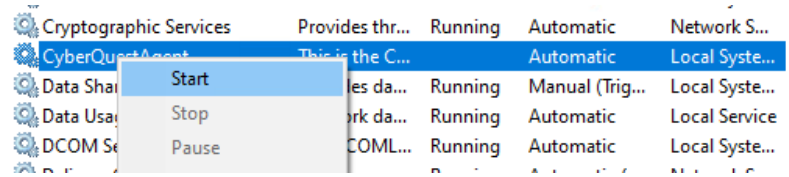
B. **Restart RabbitMQ**

We connect to the CYBERQUEST server via ssh (e.g. ssh user@ip) and restart RabbitMQ using the following command:

```
systemctl restart rabbitmq-server.service
```

C. **Start CYBERQUEST Agent**

On the Windows machine where the CYBERQUEST Agent is installed, open Windows Services and start the CYBERQUEST Agent service.



To verify that the CYBERQUEST Agent has started, open Task Manager> Details and wait until the **Agent.exe** process appears in the Task Manager.

Maintenance

Contacting Support

Requests, questions, or any inquiry can be submitted on the Nextgen Software Support Portal: **https://portal.cyberquest.cloud/ (https://portal.cyberquest.cloud/)**, in **SupportTickets** section.

Maintenance services and support

Nextgen Software offers maintenance and supports packets, designed to meet your business needs and help you maximize your software investment. With all support offering levels, you will have access to trained software support engineers.

Nextgen Software provides support in both English and Romanian languages.

Nextgen Software portal (https://portal.cyberquest.cloud/) will provide access to the following components

Support program components	Standard	Critical	Premier
Service request logging - web, telephone and e-mail	•	•	•
Service request management	•	•	•
New releases	•	•	•
Maintenance updates	•	•	•
Service packs or patches	•	•	•
Product documentation	•	•	•
Product downloads and documentation	•	•	•
Product information	•	•	•
Product notifications	•	•	•
Knowledge Base	•	•	•
Multi-media knowledge base	•	•	•
Support profile	•	•	•
Business critical hours (24x7)		•*	•*
Designated Support Account Manager (SAM)			•
Onsite visits			•**
Priority response time and service request routing			•
Proactive support and incident prioritization			•
Customized reporting			•
Personalized product communications			•
Annual discussion with Product Manager			•
" * " - Available as an option for our product. **" **** " - Available only for Romania.			

Standard Support

Standard Support is available during regular business hours for a single geographic region as defined by the support region (Americas, EMEA or Asia Pacific).

Service requests can be accessed through **https://portal.cyberquest.cloud/** (https://portal.cyberquest.cloud/) or by email at support@nextgensoftware.eu.

With the purchase of Standard Support customers receives the following elements of service:

• Ability to download the latest releases, patches, corrections, enhancements and upgrades for Nextgen Software product as they are made generally available on **https://nextgensoftware.eu/** (https://nextgensoftware.eu/).

• Access to service request logging regarding operational/technical aspects of your software by email at support@nextgensoftware.eu or by registering on the portal **https://portal.cyberquest.cloud/** (https://portal.cyberquest.cloud/).

• Ability to use online Service Request to create, update and review support cases at **https://portal.cyberquest.cloud/** (https://portal.cyberquest.cloud/).

• Access to Nextgen Software documentation on **https://docs.cyberquest.cloud/** (https://docs.cyberquest.cloud/).

• Access to the latest product information on **https://docs.cyberquest.cloud/** (https://docs.cyberquest.cloud/).

Critical Support

Customers who require 24x7 support can purchase Business Critical Support packet. This service provides 24x7 support for high priority issues as well as 24x5 support for all other issues. This means our Critical Support customers receive full 24x5 support Monday through Friday and for high priority issues support during weekends and public holidays.

Premier Support

Our highest service level offering is designed for customers with complex environments requiring a closer service relationship and a more proactive approach to support service delivery. This offering is particularly suited for customers whose business based on **Nextgen Software** product and solution.

One of the key features under Premier is the provision of a Support Account Manager (SAM). The SAM will act as a trusted advisor and will operate as an extension of your own support team, focusing on your individual business requirements.

This is a highly personalized and proactive support service for **Nextgen Software** solution. Premier Support pricings are set together with an account manager from Nextgen Software.

Service level features under Premier Support include:

• All the features included with either Standard or Critical which the Premier Support service overlays;

• A dedicated Support Account Manager;

• Access to our most experienced **Nextgen Software** Support Engineers;

• Faster response times;

• Site visits (available only in Romania) and regular activity review calls.

Support contacts and registration

Nextgen Software SRL:

• via: **https://portal.cyberquest.cloud/** (https://portal.cyberquest.cloud/) and e-mail at **support@nextgensoftware.eu** for service request logging and service request management;

• Work hours: Monday through Friday between 9:00 and 18:00, GMT+2.

Registration on Nextgen Software portal

When submitting a service request on **Nextgen Software** portal **https://portal.cyberquest.cloud/** (https://portal.cyberquest.cloud/), we assign unique service request numbers (in the format "[##CaseID##]") to all customer requests for assistance. These service request numbers allow Support to prioritize and track all service requests through resolution, and allow the customer to get a status update of their case via **https://portal.cyberquest.cloud/** (https://portal.cyberquest.cloud/) .

Service request management process

Nextgen Software portal assigns unique service request numbers (in the format **"[##CaseID##]")** to all customer requests for assistance. These service request numbers allow Support to prioritize and track all service requests through resolution, and allow the customer to get a status update of their case via **https://portal.cyberquest.cloud/** (https://portal.cyberquest.cloud/).

All service requests are assigned priorities and are placed in a queue to be processed by the next available Support Engineer. Support Engineers take ownership of your service request and see it through to successful resolution.

The Support Engineer will contact the customer, gather any additional information needed, and will investigate to determine the proper course of action. This may require the engineer to re-create the issue, work with our development team, and work with the customer on their configuration of the software.

Case logging

Prior to logging a service request you may want to review these helpful tips:

• Check the online help;

• Check the Product Documentation on **https://nextgensoftware.eu/** (https://nextgensoftware.eu/)

• Try to see if the problem is reproducible;

• Check to see if the problem is isolated to one machine or more; • Note any recent changes to your system and environment.

Contact Nextgen Software to open a service request

Submitting a service request can be done by accessing **https://portal.cyberquest.cloud/** (https://portal.cyberquest.cloud/). Requests for technical assistance can also be sent via e-mail to **support@nextgensoftware.eu**.

Service Request priorities and response times

All service requests register at **https://portal.cyberquest.cloud/** (https://portal.cyberquest.cloud/) or by e-mail **support@nextgensoftware.eu** are assigned priorities based on the impact on your business. The customer determines the initial priority when placing a request for assistance. Priorities may be changed after initial contact and assessment of the issue from our support engineer. The following table defines the priorities and the targeted initial response time for Standard and Premier Support.

Priority	Description	Initial response Standard	Initial response Premier	Initial response Critical
High	**Critical business impact:** Customer's production use of our product on primary business service, major application or mission critical system is stopped or so severely impacted that the customer cannot reasonably continue work. For high priority problems, we will begin work on the problem within one hour of notification and handle as its highest priority until the customer is given a fix or workaround. Customer resources must be made available in high priority situations and reasonably cooperate to resolve the issue. **High priority problems could have the following characteristics:** `system hangs or crash situations` `•Data loss or data corruption` `•Critical functionality not available / High priority issues must be reported via telephone`	Within 6 hours	Within 3 hours	Within 3 hours

Note: High priority service requests must be logged through e-mail at support@nextgensoftware.eu or on the portal https://portal.cyberquest.cloud/ (https://portal.cyberquest.cloud/)

Priority	Description	Initial response Standard	Initial response Premier	Initial response Critical
Medium	**Significant business impact:** Important product features are unavailable with no acceptable work-around. Customer's implementation or production use of our product in a primary business service, major applications or mission critical systems are functioning with limited capabilities or are unstable with periodic interruptions. The software may be operating but is severely restricted. **Medium problems could have the following characteristics:** `•Product error or failure forcing a restart or recovery` `•Severely degraded performance` `•Functionality unavailable but the system is able to operate in a restricted mode`	Within 12-24 hours	Within 12 hours	Within 12 hours

Priority	Description	Initial response Standard	Initial response Premier	Initial response Critical
Low	**Minimal business impact:** Product features unavailable but a workaround exists and the majority of software functions are still useable. Minor function/feature failure that the customer can easily prevent or avoid. Customer's work has minor loss of operational functionality. Also, minor problem or question that does not affect the software function such as how to's documentation, general questions or enhancement requests. There is no impact to product usage or customer's operations. **Low priority problems could have the following characteristics:** `•Error message with workaround` `•Minimal performance degradation` `•Incorrect product behavior with minor impact` `•Questions on product functionality or configuration during implementation` `•General requests for advice on product usage` `•Clarification on product documentation or release notes` `•Product enhancement request`	Within 48 hours	Within 24 hours	Within 24 hours

Closing a service request

Requests for support (Service Requests) remain open until the customer is satisfied that the request can be closed. Exceptions to this policy apply to requests for product enhancements.

Re-opening service request

Customers can re-open service requests that have been closed within 30 days of the close date. Customers have the ability to re-open their closed service requests from the "My Requests" section of **https://portal.cyberquest.cloud/** (https://portal.cyberquest.cloud/) portal or by sending an e-mail at support@nextgensoftware.eu specifying the support technician that managed the case.

Product enhancements

Customers interested in submitting product enhancement requests can do so either via **https://portal.cyberquest.cloud/** (https://portal.cyberquest.cloud/) or by creating a service request at support@nextgensoftware.eu. For enhancements submitted by creating a case at **https://portal.cyberquest.cloud/** (https://portal.cyberquest.cloud/), once documented, the identification number will be provided to the submitter, and the support case will be closed.

Product Management will review the open enhancement requests on a periodic basis and consider them for inclusion in a future product release. Product enhancements will not be considered or implemented in current or prior product releases. There is no guarantee that a specific enhancement request will be implemented in a future version of Nextgen Software product.

Product licensing

Nextgen Software product has license keys generated for their use. Some product requires a new license key when upgrading our software to a new release and/or patch. We also recommend that prior to any migration or upgrade of our product new licenses are confirmed as functioning properly as some license keys are machine and machine-name specific.

Product Support Lifecycle

Nextgen Software "Product Support Lifecycle"

The **"Product Support Lifecycle"** describes the phases during which Nextgen Software product are eligible for patches (fixes), support and downloads from our support portal.

It is Nextgen Software policy to provide support and fixes in last versions of the software to supported customers; fixes to older versions are at Nextgen Software discretion.

We will attempt to answer questions on older versions of Nextgen Software product provided resources are available; however, we encourage customers using discontinued versions to upgrade to the currently supported version of the software.

Nextgen Software's usual support policy is to provide support on both the current (n) and prior (n-1) versions of our product.

Product Version Numbering

Each Product release is identified with a numerical version comprising three sets of digits separated by decimals. The digit(s) to the left of the first decimal represent the major version, the digit(s) to the right of the first decimal represent the minor version, and the digit(s) to the right of the second decimal represent the maintenance version. Any version number that specifies the second digit(s) is referred to as a minor version, even if it is the first release of a new major version. For example, 2.0, 2.11, and 2.15 are all minor versions of the 2.x major version.

Any given Product version is considered a Supported Version ("Supported") for a finite period following its release. Note that any prior version of any of these Products not listed here is End of Support.

Once a Product version is no longer Supported, it is considered End of Support. End of Support Product versions are not eligible for Support Services, and any software, associated product documentation will no longer be available to Customers.

"Product Support Lifecycle" Phases

Version	Release Date	Support phase*	End of Support
2.0.5	Nov 2017	Discontinued	Oct 2020
2.11	Apr 2018	Discontinued	Mar 2021
2.15	Sep 2019	Limited support	Aug 2022
2.20	Jul 2021	Full support	Jun 2024
2.30	Feb 2023	Full support	Jan 2027

Full support

• Product is fully supported, generally available release/version;

• Includes the most current released version of a product and could be one prior releases;

• Enhancement requests for this release are accepted and may be considered for future releases;

• Maintenance releases and/or hotfixes are periodically made available for this release;

• Release/version is fully supported by both Support and Development;

• Release/version is available for download from **https://nextgensoftware.eu/** (https://nextgensoftware.eu/).

Limited support

• Support is available for this release/version, and we will use best efforts to provide known workarounds or fixes;

• No new code fixes will be generated except under extreme circumstances and at our discretion;

• Enhancement requests are not accepted;

• Customers are encouraged to plan an upgrade to a release/version on full support;

Discontinued

• Includes release/versions which are not supported/discontinued;

• No new patches or fixes will be created for this release;

• Support will be provided as upgrading documentation to a supported version;

• Support is not obligated to provide assistance on this version of the product.

Editions

On prem

AIO

The AIO instance (All-In-One) is the first choice for most projects for it's straight forward installation and configuration process. In this configuration, all the components and services of CYBERQUEST are residing on a single machine.

We recommend the AIO deployment for it's stability, ease of configuration and operation.

This version is most suitable for deployment in small to medium IT infrastructures.

Distributed edition

By distributed edition (distributed architecture) we understand that CYBERQUEST can be deployed on multiple machines, in the same network or in different networks.

In the distributed architecture, CYBERQUEST can be deployed as AIO on multiple machines (for HA purposes etc.), or CYBERQUEST's component services are deployed on separate machines.

The main purpose for configuring CYBERQUEST in a distributed architecture is increase in performance by distributing load on multiple machines. Though it is very tempting for the consistent increase in performance, it is subject to increased service demands (due to the complexity of the instance) and third party software or hardware failures have a greater impact.

We recommend distributed architecture only for large projects, and we specifically design the solution for each such project.

Scaling Online DataStorage

This is done by deploying the Online DataStorage service on a separate machine. By usage of separate processing power for maintaining the NoSQL data repository, high ingestion (in EPS) and correlation values may be reached per CPU for the CYBERQUEST processing server.

For large amounts of data (above 5TB) an Online DataStorage cluster can be deployed. See chapter.DataStorage clustering.

Scaling Data Server

In some instances, where data must be collected from separate (and, in many cases, also remote) networks, the Data Server service (responsible with receiving the streams of data) can be deployed on separate machines. Also, the scaling of Data Server can be done for overall performance increase.

Scaling Rabbit MQ

By deploying the queueing service (powered by RabbitMQ) on separate machines the overall performance of the CYBERQUEST instance can be increased.

Scaling Data Storage (Archive)

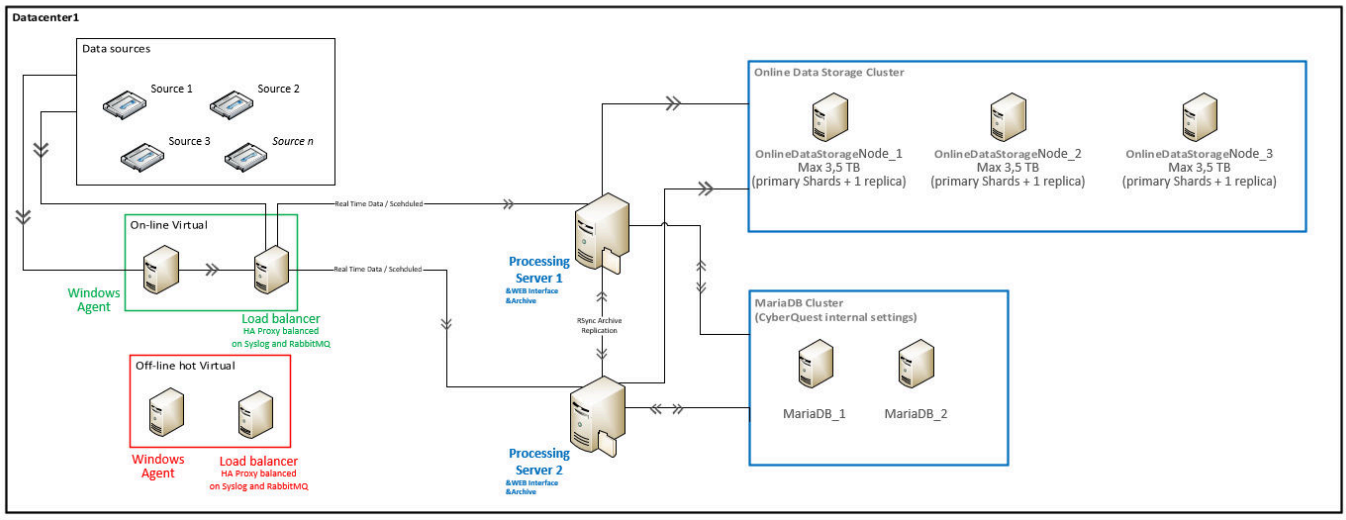
In projects where data must be retained for extra long periods of time and with requirements of immediate access, the Data Storage service can be deployed on separate machines. This enables CYBERQUEST to maintain huge archive repositories. It also provides some increase in the overall performance of the CYBERQUEST instance.

Scaling Correlation Engine

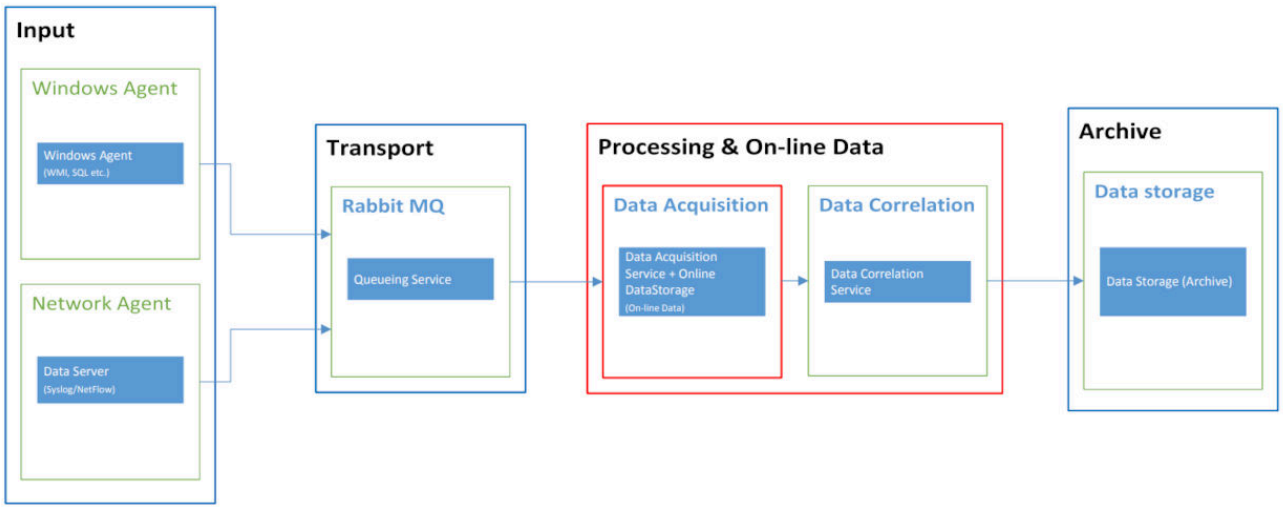
Scaling the Correlation Engine, besides the Online DataStorage service, is the most performance increase scaling that can be implemented for a CYBERQUEST instance.

Examples

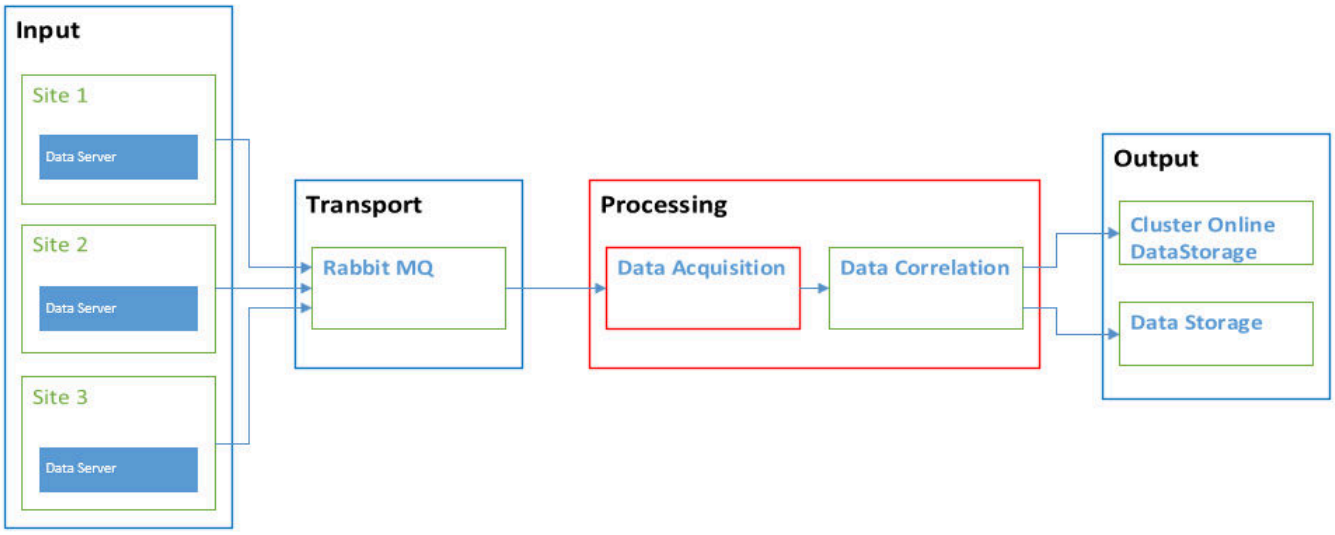
High availability deployment (variant)



Distributed architecture with Online DataStorage included



Distributed architecture with Online DataStorage distributed and multiple site collection



CYBERQUEST Licensing and Versioning

CYBERQUEST is available both as a free edition or as a commercial edition. The commercial editions are: **Logger, Light**, **Advanced**, **Enterprise** and **Ultimate**. The table below details the features of each edition:

Description / version	Free	Logger	Light	Advanced	Enterprise	Ultimate
Users limit	1	3	5	10	20	Unlimited*
Included cores	4	4	4	6	8	1**
Included EPS	250	250	500	750	1000	Unlimited*
Daily GB of data	1	2	10	160	600	Unlimited*
CPU cores/instance	4	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
Dashboards	yes	yes	yes	yes	yes	yes
Custom dashboards	no	no	yes	yes	yes	yes
Dashboards per dashgroup	6	9	12	15	24	Unlimited*
Dashgroups per instance	2	4	6	10	16	Unlimited*
Data permissions-no. of filters	×	×	2	10	Unlimited*	Unlimited*
Short term Data Storage (days)	15	30	30	90	Unlimited*	Unlimited*
Long term Data Storage (days)	×	×	365	730	Unlimited*	Unlimited*
Max. no. of Online DataStorage Nodes/instance	1	1	2	3	Unlimited*	Unlimited*
Max. no. of DTS Objects	4	6	10	15	Unlimited*	Unlimited*
Geolocation	☑	☑	☑	☑	☑	☑
Reports	☑	☑	☑	☑	☑	☑
Compliance Reports	☑	☑	☑	☑	☑	☑
Asset Management	×	×	×	☑	☑	☑
Windows Agent Collection	☑	☑	☑	☑	☑	☑
ODBC Data Collection	☑	☑	☑	☑	☑	☑
Syslog Data Collection	☑	☑	☑	☑	☑	☑
NetFlow Data Collection	×	×	×	☑	☑	☑
NetFlow Stitching	×	×	×	×	☑	☑
Multiple Data server for advanced technologies	×	×	×	☑	☑	☑
MultiTenancy	×	×	×	×	×	☑
Simple Alerts (1 step rules)	×	×	20	50	Unlimited*	Unlimited*

Description / version	Free	Logger	Light	Advanced	Enterprise	Ultimate
Correlated Alerts (multi step rules)	✗	✗	5	20	Unlimited*	Unlimited*
Summary Alerts	✗	✗	✗	20	Unlimited*	Unlimited*
Add-on 2, 4 or 8 Cores-extra fee	✗	☑	☑	☑	☑	☑
Add-on 1GB, 5GB, 10GB or 100 GB/day-extra fee	✗	☑	☑	☑	☑	n/a

*__No limit is set in the license for the number of integrated IT&C devices/data sources. Performance and processing capacity depend on the allocated hardware resources__

**__The license is for 1 CPU. Minimum numbers of license cores that can be purchased is 8 and the estimated performance is about 1800 EPS__

How CYBERQUEST license works

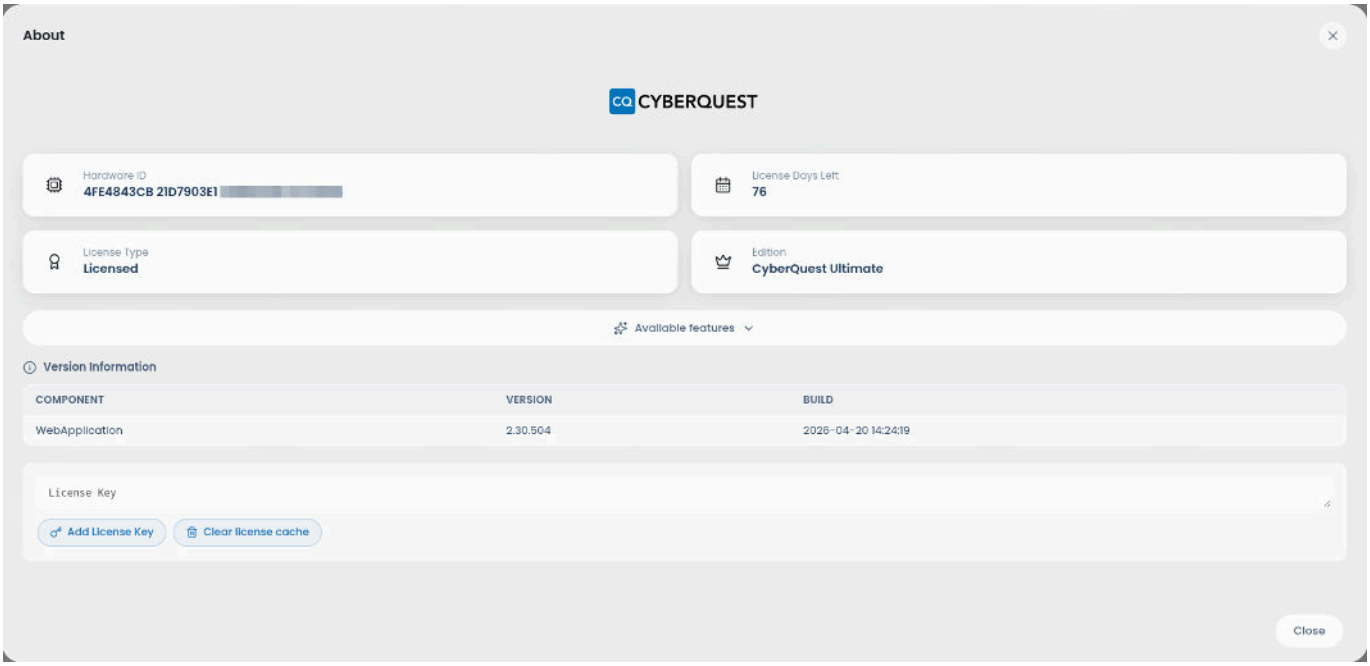
A short description of each criteria subject to license can be found below:

- **Max. no. of users** is the maximum number of active users the solution allows
- **No. of cores included**: the solution runs on a standalone machine based on Linux Debian 13/CYBERQUEST OS/ RedHat 10 operating system. The number of CPU cores included in license represents the maximum number of CPU cores of the system where CYBERQUEST runs
- **Up to no. of EPS included**: is the maximum number of events per second the solution can process and is calculated mostly by the number of CPU cores, but also the hardware capabilities of the system
- **Max Data per day GB**: depending on instance configuration, represents the maximum quantity of data the solution can process, according to your license.
- **Max number of CPU Cores per instance**: is the maximum number of CPU cores which can be licensed for a CYBERQUEST instance. It can be increased by adding licenses for more CPU cores (add-ons)
- **Dashboards**: notifies if the selected edition has access to **Dashboards** functionality in CYBERQUEST
- **Custom Dashboards**: notifies if the selected edition has access to editing and creating dashboards by platform users
- **Max number of active Dashboards per Dashgroup**: notifies on the maximum number of dashboards that can be active in a dashgroup for the selected edition
- **Max number of Dashgroups**: represents the maximum number of groups which can be active in an instance
- **Data Permissions: number of filters**: notifies on the permission to apply filters on data processed by CYBERQUEST, as well as the number of filters on which the licensing allows
- **Short Term Data Storage (days)**: depending on the storage capacity, represents the maximum number of days allowed by license, for which data can be stored in the online database
- **Long Term Data Storage (days)**: depending on the storage capacity, represents the maximum number of days allowed by license, for which data can be stored in the offline database, and if archiving is allowed by license
- **Max number of Online DataStorage Nodes per instance**: is the maximum number of Online DataStorage nodes allowed by license to be attached to a CYBERQUEST instance
- **Max number of DTS Objects**: is the maximum number of active objects allowed by license in CYBERQUEST's Data Transformation Services module.
- **Geolocation**: notifies if the selected edition has access to geolocation functionality in CYBERQUEST

- **Reports**: notifies if the selected edition has access to **Reports** functionality in CYBERQUEST
- **Compliance Reports**: notifies if your license activates also the built-in compliance reports to standards
- **Asset Management**: refers to inventorying capability in CYBERQUEST being active or not within your license
- **Windows Agent Collection**: notifies if the selected edition can use Windows Agent-based gathering
- **ODBC Data Collection**: notifies if the selected edition can use ODBC-based gathering
- **Syslog Data Collection**: notifies if the selected edition can use syslog-based gathering
- **NetFlow Data Collection**: notifies if the selected edition can use NetFlow gathering
- **NetFlow Stitching**: notifies if the selected edition can pair send and receive events for TCP/IP communication and forming a unified event in this process
- **Multiple Data Server for advanced topologies**: represents the ability to deploy multiple Data Server instances in order to collect data from various network segments
- **MultiTenancy**: represents the ability to run multiple clients on the same instance
- **Simple Alerts (1 step rules)**: notifies if the selected edition can use, and the maximum number allowed, for single step alerts
- **Correlated Alerts (multi-step rules)**: notifies if the selected edition can use, and the maximum number allowed, for multiple step alerts
- **Summary Alerts**: notifies if the selected edition can use, and the maximum number allowed, for summary alerts

Depending on the licensing model you choose, there are also restrictions on the available connectors, nodes and various configuration objects.

To access Licensing module, go to **Settings** > **About**. **About CYBERQUEST** window opens containing information about your accessed instance.



Available information in the **About CYBERQUEST** window is:

- Hardware ID - Unique hardware ID of CYBERQUEST machine and for which permanent license is issued
- License days left - information about the number of days for license availability
- License type - notifying if your product is licensed, under grace period or not licensed
- Edition - platform edition for which the license was registered

The window also contains version and build date for each component module.

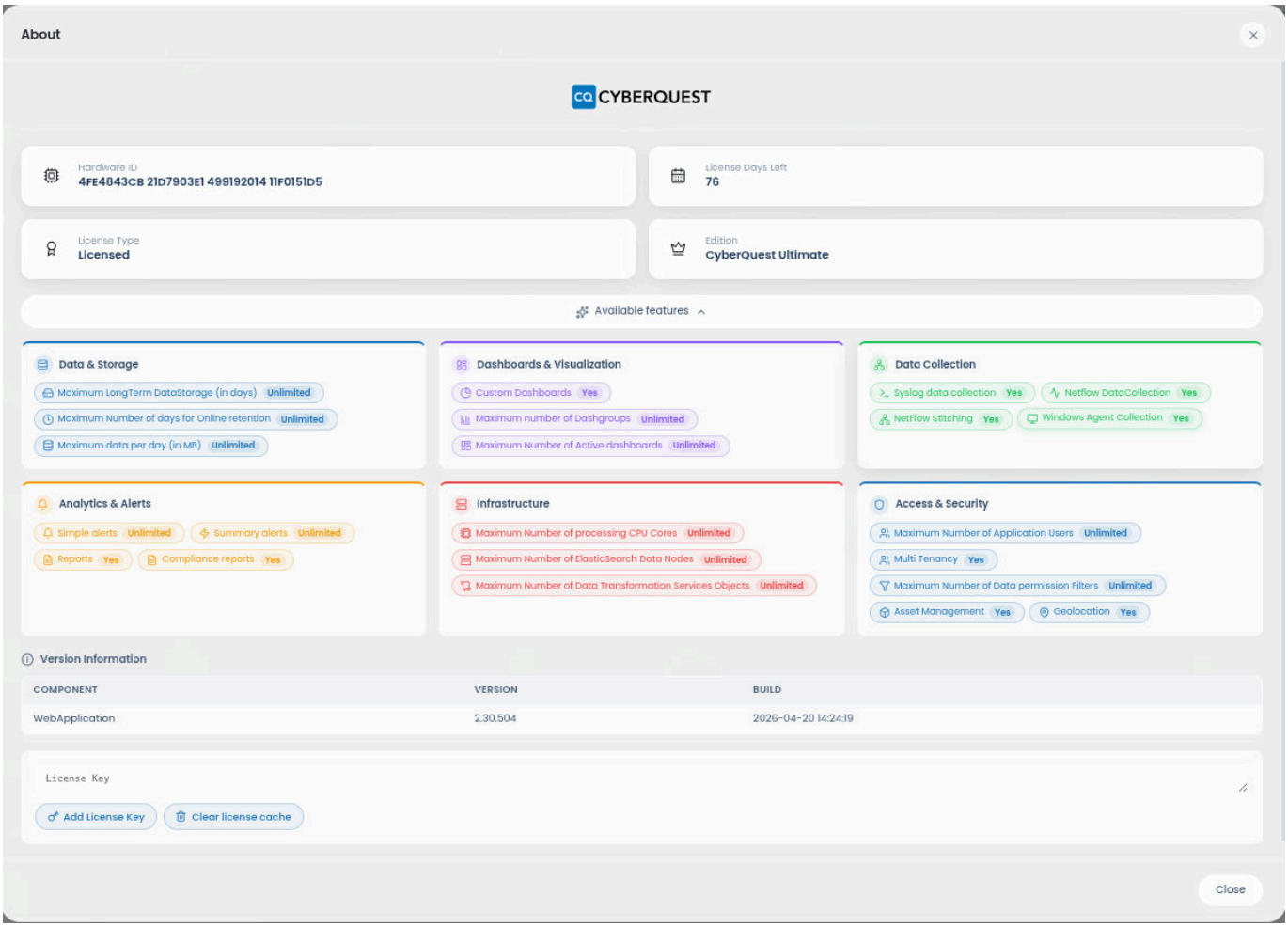
A new license key can be pasted into **License Key** field and applied by pressing **Add License Key** button. An added license can either replace the current license, or provide additional functionalities like with add-on licenses.

The **Clear license cache** button forces the update of the license details in the web interface.

Click



to display detailed information about your license.



CYBERQUEST in Practice

Operational

Service Parameters

Data Server

Service parameters which are found in service configuration files:

parameter	type	default value	description
compressData	boolean	true	Message compression flag
encryptData	boolean	true	Message encryption flag
throttleCollection	string	“100000”	Number of events stored in the message queue at which it will stop sending events. All events will be cached locally
mqHost	string	“127.0.0.1”	Address of the queuing services
mqPort	string	“5672”	Port of the queuing services
mqUserName	string	“cq”	Username of the queuing services
mqPassword	string	“*******”	Encrypted password of the queuing services
mqUseSSL	boolean	false	Whether use tls queue services
tenant	string	""	Tenant name
useHTTPSTransport	boolean	false	Whether use https transport instead of message queue service
HttpTransportUrl	string	“127.0.0.1”	Https transport url
CLIENT_ACCESS_TOKEN	string	“DEFAULT_CLIENT-ACCESS-TOKEN”	Https transport access token
UDPSyslogPort	string	“5140”	UDP syslog server port with process of data
UnprocessedUDPSyslogPort	string	“5141”	UDP syslog server port without process of data
TCPSyslogPortEn	boolean	true	TCP syslog server enable flag
TCPSyslogPort	string	“32004”	TCP syslog server port with process of data
UDPNetflowPort	string	“2055”	UDP netflow capture server port
UDPCEFPort	string	“5142”	UDP CEF format server port
UDPIntrustPort	string	“5143”	UDP intrust format server port
UDPListenIP	string	“0.0.0.0”	IPv4 Address For UDP servers to listen
CacheMinimumFreeSpace	string	“2048”	Minimum space available on disk to write data, in case of throttling
MaximumContainerValue	string	“500000”	Maximum data stored in container, if flodded udp port data will be discarded and alert will be given
debugLevel	string	“0”	The debug level as 0-FATAL ERROR,ERROR messages 1-WARNING messages 2-INFO messages 3-DEBUG messages
UDPSyslogPortEn	boolean	false	UDP syslog server port with process of data enable
UnprocessedUDPSyslogPortEn	boolean	false	
UDPNetflowPortEn	boolean	false	UDP netflow capture server enable
UDPCEFPortEn	boolean	false	UDP CEF format server enable
UDPIntrustPortEn	boolean	false	UDP intrust format server enable

Data Acquisition

Service parameters which are found in service configuration files:

```
config.ini file
```

parameter	type	default value	description
Alternate_DB_HOST	string	tcp://127.0.0.1:3306	This is the address of the alternate mysql DB server
Config_DB_HOST	string	tcp://127.0.0.1:3306	This is the address of the mysql DB server
Config_DB_DB	string	config	This is the database name of the mysql DB server
Config_DB_USER	string	root	This is the username of the mysql DB server
Config_DB_PASSWORD	string	****	This is the password of the mysql DB server

The following are parameters set in application settings:

parameter	type	default value	description
EL_Url	string	127.0.0.1	Short term storage (Online DataStorage) address
EL_Port	string	9200	Short term storage (Online DataStorage) port
LIC_PATH	string	/var/opt/cyberquest/dataacquisition/conf/lic	License file path
CLEANUP_CRON	string	* * * * *	**deprecated**
bulk_size	string	2000	Bulk size to send to short term storage (Online DataStorage)
no_of_threads	string	3	**deprecated**
ServiceDebugLevel	string	2	The debug level as 0-FATAL ERROR,ERROR messages 1-WARNING messages 2-INFO messages 3-DEBUG messages
RMQ_host	string	127.0.0.1	Address of the queuing services
RMQ_username	string	cq	Username of the queuing services
RMQ_password	string	********	Encrypted password of the queuing services
RMQ_queue	string	events	Queuing services incoming events queue name
maxmindb_path	string	/var/opt/cyberquest/dataacquisition/bin/GeoIP.mmdb	Location of maxmindb database file
run_collection_servers	boolean	false	**deprecated**
throttle_queue	string	100000	Number of events stored in the message queue at which it will stop sending events. All events will be cached locally.
cache_path	string	/data/dataacquisition/cache/	Cache files location
collection_unique_keys	string	Computer,EventLog,agent_guid	Unique event identifier based of fields enumerated, to identify one asset
el_shards	string	2	Template number of shards for short term storage
use_http_ES_DA_client	string	1	Whether use http transport for Short term storage (Online DataStorage), if false transport will be used by other means via queue service (fanout)
sendRawData	string	0	Whether send raw data to short term storage (Online DataStorage)
writeEventPath	string	0	Whether send path of the event in CQ system to short term storage (Online DataStorage)
validateDataForEL	string	1	**deprecated**
GetterThreadNo	string	3	Number of threads to read from incoming events queue
ParserThreadNo	string	3	Number of threads to parse data
RMQPusherThreadNo	string	2	Number of threads to push data to queue service
ELPusherThreadNo	string	2	Number of threads to push data to short term storage (Online DataStorage)
supressRawData	string	1	Whether delete raw data to send to long term storage (datastorage)
RedisServerURL	string	127.0.0.1	Memory based storage address

parameter	type	default value	description
RedisServerPORT	string	6379	Memory based storage port
ResyncCache	string	0	Resync cache if used in default parsers, it will be reset to 0 after setting it to 1
UseDefaultParsers	string	1	Whether use internal defined parsers for all events
EL_minim_free_space	string	3072	Minimum space available on disk used by short term storage (Online DataStorage), in case of throttling
Cache_minim_free_space	string	3072	Minimum space available on disk to write data, in case of throttling
LoadDatabase	string	false	Whether load database stored in sql folder
debug_level	string	1	The debug level as 0-FATAL ERROR,ERROR messages 1-WARNING messages 2-INFO messages 3-DEBUG messages

Data Correlation

Service parameters which are found in service configuration files:

```
config.ini file
```

parameter	type	default value	description
Alternate_DB_HOST	string	tcp://127.0.0.1:3306	This is the address of the alternate mysql DB server
Config_DB_HOST	string	tcp://127.0.0.1:3306	This is the address of the mysql DB server
Config_DB_DB	string	config	This is the database name of the mysql DB server
Config_DB_USER	string	root	This is the username of the mysql DB server
Config_DB_PASSWORD	string	***	This is the password of the mysql DB server

The following are parameters set in application settings:

parameter	type	default value	description
AplicationGUID	string	334CFC20-F2D3-A7D1-D3B7-DBB79ED69B5C	This is the Server global unique ID , is represented by 32 lowercase/uppercase hexadecimal digits, displayed in five groups separated by hyphens, in the form 8-4-4-4-12 for a total of 36 characters
EL_Url	string	127.0.0.1	Short term storage (Online DataStorage) address
EL_Port	string	9200	Short term storage (Online DataStorage) port
DebugLevel	string	2	The debug level as 0-FATAL ERROR,ERROR messages 1-WARNING messages 2-INFO messages 3-DEBUG messages
RMQueueAddress	string	127.0.0.1	Address of the queuing services
RMQueuePort	string	5672	Port of the queuing services
RMQueueUserName	string	cq	Username of the queuing services
RMQueuePassword	string	********	Encrypted password of the queuing services
RMQueueName	string	DataCorrelation	Queuing services incoming events queue name
throttle_queue	string	100000	Number of events stored in the message queue at which it will stop send events. All events will be cached locally
cache_path	string	/data/datacorrelation/cache/	Cache files location
RedisServerURL	string	127.0.0.1	Memory based storage address
RedisServerPORT	string	6379	Memory based storage port
restart	bool	0	Restarts data correlation service
PercolatorThreadPoolSize	string	3	Threadpool for percolator
PercolatorNumberOfContainers	string	1	Number of containers to be used to percolate

Data Storage

Service parameters which are found in service configuration files:

```
conf.xml file
```

parameter	type	default value	description
dbDriver	string	com.mysql.jdbc.Driver	This is the driver of the mysql DB server
dbUserName	string	root	This is the username of the mysql DB server
dbPass	string	****	This is the password of the mysql DB server
dbUrl	string	jdbc:mysql://127.0.0.1:3306/config	This is the address of the mysql DB server
dbAlternateUrl	string	jdbc:mysql://127.0.0.1:3306/config	This is the address of the alternate mysql DB server
serverGuid	string	D39498A9-1C85-0379-1E78-C161E6FFEEEA	This is the Globally Unique IDentifier(GUID) of server

The following are parameters set in application settings:

parameter	type	default value	description
maxEventsPerFile	string	20000	Specifies the maximum number of events allowed per stored file
fileWriterTimeout	string	60	Specifies the timeout interval for the event writer
mqUserName	string	cq	Specifies the administrative username for MQ service access
mqPassword	string	****	Specifies user's password for MQ service
mqHost	string	127.0.0.1	Specifies the MQ service server. In distributed architectures, it may differ from the default CYBERQUEST server
mqVhost	string	/	Specifies the MQ service virtual server. In distributed architectures, it may differ from the default CYBERQUEST server
mqPort	string	5672	Specifies the network communication port used by MQ service
mqExchangeName	string	eventsExchange	Specifies the exchange name used by MQ service
mqQueueName	string	jobCommands	Specifies the MQ queue name
mqReceiveQueueType	string	fanout	Specifies the MQ Receive queue type
mqRouting	string	agents	Specifies the routing path for message queues
mqReceiveCommandExchangeName	string	eventsExchange	Specifies the MQ Receive command exchange name
mqReceiveCommandQueueName	string	jobCommands	Specifies the MQ Receive command queue name
mqReceiveCommandQueueType	string	direct	Specifies the MQ Receive command queue type
mqReceiveCommandRouting	string	servers	Specifies the MQ Receive command routing path
mqSendExchangeName	string		Specifies the MQ Send exchange name
mqSendQueueName	string	archive	Specifies the MQ Send queue name
mqSendRouting	string	agents	Specifies the MQ Send routing path
mqSendQueueType	string	direct	Specifies the MQ Send queue type
encryptionPublicKeyFilePath	string	/var/opt/cyberquest/ encryption/datastorage/ public_key.txt	Specifies the file path for defined public key
encryptionPrivateKeyFilePath	string	/var/opt/cyberquest/ encryption/datastorage/ private_key.txt	Specifies the file path for defined private key
elasticClusterName	string	ES.	Specifies the Online DataStorage cluster name
elasticHostName	string	127.0.0.1	Specifies the Online DataStorage host name
encryptionPrivateKeyPassword	string	***	Specifies the password for defined private key
encryptionPrivateKeyPasswordPath	string	/var/opt/cyberquest/ encryption/datastorage/ privateKeyPassword.txt	Specifies the file path for defined private key password
fileImportThreads	string	5	Specifies how many threads are used for import
mqQueueType	string	direct	Specifies the queue type
mqReceiveExchangeName	string	DA.publish	Specifies the MQ Receive exchange name
mqReceiveQueueName	string	DataStorage	Specifies the MQ Receive queue name
mqReceiveRouting	string	agents	Specifies the MQ Receive routing key

parameter	type	default value	description
mqAlternateHost	string	127.0.0.1	Specifies the alternate host name to use if the current queue is dead
mqVHost	string	/	Specifies the MQ Receive virtual host

Windows Agent

You can find all configurable variables in the following table:

parameter	type	default value	description
eventSyncQueueSize	integer	10000	Number of events sent every 5 seconds
compressData	boolean	true	Compress event data or not
encryptData	boolean	true	Encrypt event data or not
cleanupOlderLogsDays	integer	7	Automatic cleanup on agent logs
throttleCollection	integer	10000	Threshold at with it will gradually start to collect less events (this value is given by how many messages are waiting in the CYBERQUEST processing server queue)
mqHost	string	192.168.200.128	CYBERQUEST server host
mqUserName	string	cq	CYBERQUEST server username
mqPassword	string	****	Hash of the CYBERQUEST server password
HttpTransportUrl	string	false	Used for cloud deployments and url for sending data to the CYBERQUEST server cloud
CLIENT_ACCESS_TOKEN	string	false	Authentication token for the CYBERQUEST server cloud
mqUseSSL	boolean	false	Use encrypting on the whole connection to the CYBERQUEST server or not

Alerts create logon config

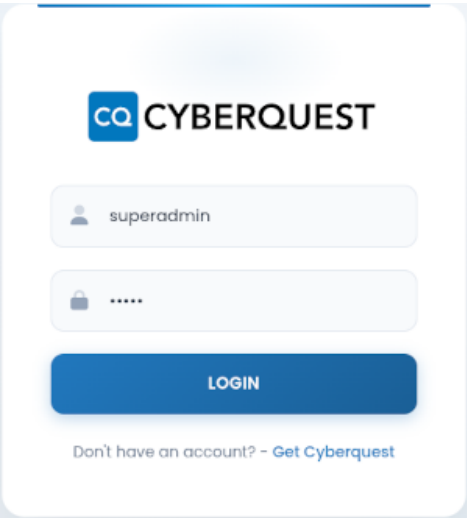
CYBERQUEST's **alerting module** is fully customizable for each connected user. Alerts can be **triggered by user-defined events**, allowing the system to respond precisely to specific scenarios.

This flexibility ensures **high accuracy** and helps **minimize false alerts**, providing reliable notifications tailored to each user's needs.

Authentication

To access the CYBERQUEST Web Interface:

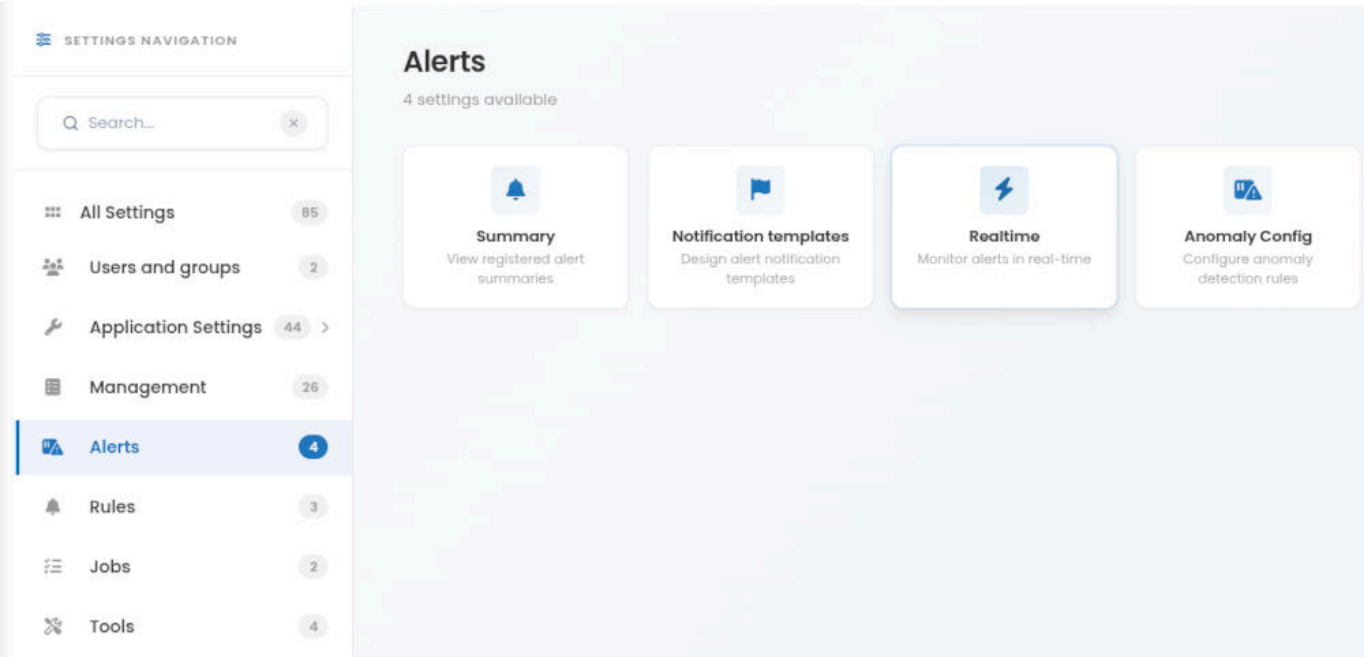
- Open a web browser and navigate to the application's address or DNS name
- The default address format is: ***https://CyberquestIPAddress*** (replace with the actual IP address)
- The browser will redirect automatically to the CYBERQUEST authentication page.



Note: Valid credentials with the appropriate permissions are required to create and manage alerts.

Navigate to Alerts Module

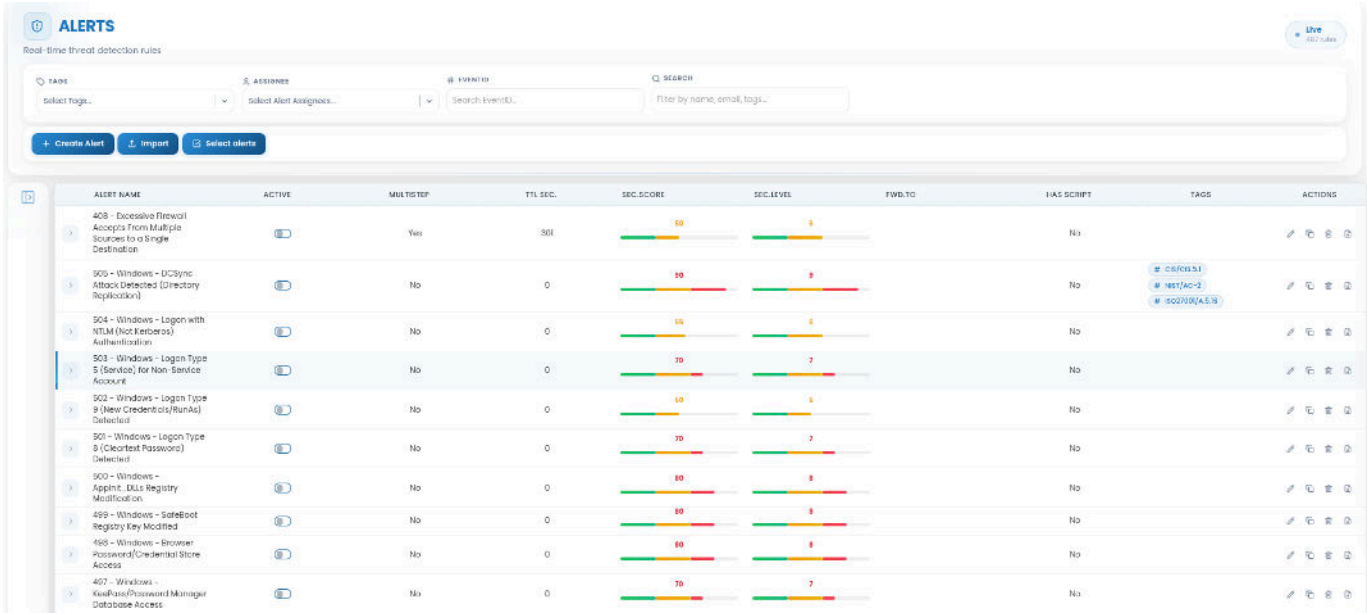
- From the main navigation menu, click on **Settings**
- In the Settings menu, select **Alerts > Realtime**
- The Realtime Alerts page will open, displaying all existing alert definitions



The Realtime Alerts page provides options to view, edit, delete, and create alert definitions. Each alert can be customized to meet specific security requirements.

Create New Alert Definition

- On the Alerts page, locate and click the **"CREATE ALERT"** button
- This opens the alert configuration interface for defining a new alert.

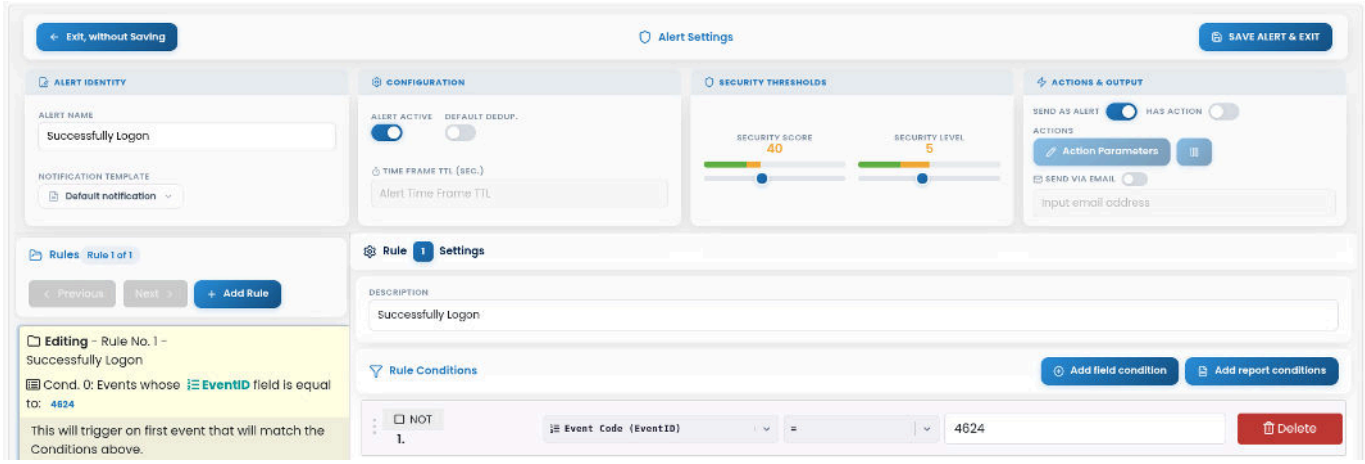


Clicking this button opens a comprehensive configuration form to specify alert parameters, rules, and notification settings.

Configure Alert Settings

The alert configuration interface provides several key sections:

Basic Alert Configuration



Alert Name: Enter a descriptive name that clearly indicates the alert's purpose

Alert Active: Selecting the **Alert Active** checkbox enables the alert, while clearing it deactivates the alert without deleting it. Disabled alerts remain in the system but do not trigger notifications.

Sent as Alert: The **Sent as Alert** checkbox functions similarly to the **Alert Active** option. When unchecked, the alert remains active but does not generate visible notifications. This setting allows backend processing and correlation of anomalies across multiple events, triggers, and alerts.

Has Action: The **Has Action** checkbox enables the association of a script with the alert. After selecting it, press the **Action Parameters** button to open the **Script Editor**, where a custom script can be created and applied as a rule for the alert.

Notification Template: The **Notification Template** allows selection of either built-in or custom templates for alerts. The **Default** template provides standard formatting, while custom templates can be created to suit specific audiences or use cases.

Rule Settings: The **Rule Settings** pane provides tools for defining alert logic. Rule logic consists of **field, report, and correlation conditions** linked using the logical operators **AND, OR, and NOT**.

- **Description**: Provide a clear, concise description of what the rule monitors

- **Add Field Condition**: The **Add Field Condition** option allows specifying a condition based on an event field. Select a field (e.g., EventID, UserName, SrcIP), choose a comparison operator (equals, contains, greater than, etc.), and enter the value to match.
- **Add Report Condition**: The **Add Report Condition** option allows using an existing report as a condition. This is useful for applying pre-defined, complex queries within alert logic.
- **Delete**: Remove individual rule conditions that are no longer needed

When adding a rule condition, a **logical operator** is automatically applied to connect it with the previous condition. The default operator is **AND**, which can be toggled to **OR** by clicking the operator button. Clicking again switches it back to **AND**.

If needed, a **NOT** operator can be applied using a checkbox. By default, **NOT** is unselected; click the checkbox to apply the operator and invert the condition.

- **AND**: All conditions must be met for the alert to trigger
- **OR**: Any condition can trigger the alert
- **NOT**: Excludes specific conditions

After configuring an alert, review all settings and click **Save Alert & Exit** to save the alert definition. The alert will appear in the **Alerts** list.

Back-up CQ

Back-up CQ

MySQL database dump

Most of application configurations for CYEBRQUEST is stored in the internal MySQL database.

The database is backed up using a MySQL dump script:

```
DATE=date +%Y-%m-%d

mkdir -p /data/mysqlbackups/

mysqldump -u [dbuser] -p[dbpass] --all-databases | gzip > /data/mysqlbackups/$DATE.sql.gz
```

Replace **[dbuser]** and **[dbpass]** with MySQL username and password respectively.

This script is executed daily on a cronjob basis.

To check if the script is added to crontab scheduler use the following command:

```
crontab -l
```

The following line needs to be present:

```
30 2 * * * /var/opt/cyberquest/dataacquisition/bin/mysql_full_backup.sh
```

If it is not, then it can be added using the following command:

```
crontab -e
```

a. Paste the line on last row:

```
30 2 *** /var/opt/cyberquest/dataacquisition/bin/mysql_full_backup.sh
```

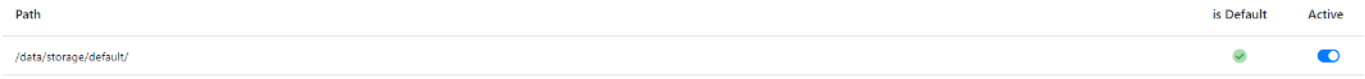
b. Save and exit

c. Finally, check **/data/mysqlbackups/** folder for backed up database presence

Event data backup

By default, every message collected by CYBERQUEST is automatically sent to data storages, as configured in **Settings > Data Storages** page:

Default: /data/storage/default



Stored events are normalized in JSON format, compressed, encrypted and digitally signed.

They can be later imported to a backup storage. In order to achieve that, follow these steps:

a. Create a new data storage as described in chapter **Managing Repositories | Configuring data storages**

b. Create an import job as described in chapter **Managing Jobs | Creating a new job**

c. Select the newly created data storage as target

Integration with third-party backup solutions

In either deployment configuration (physical appliance, virtual appliance, installable software), CYBERQUEST allows external connections to be set for data extraction and backup.

The appliance is built on Linux Debian operating system, and each platform layer can be backed up following vendor practices for:

- Backing up Linux operating systems
  - https://wiki.debian.org/BackupAndRecovery (https://wiki.debian.org/BackupAndRecovery)
  - https://debian-handbook.info/browse/stable/sect.backup.html (https://debian-handbook.info/browse/stable/sect.backup.html)
- Backing up MySQL Databases
  - https://dev.mysql.com/doc/refman/5.5/en/backup-and-recovery.html (https://dev.mysql.com/doc/refman/5.5/en/backup-and-recovery.html)
- Backing up Apache Web Server
  - http://directory.apache.org/apacheds/basic-ug/1.6-backup-restore.html (http://directory.apache.org/apacheds/basic-ug/1.6-backup-restore.html)
- Backing up Online DataStorage
  - https://opensearch.org/docs/1.2/opensearch/snapshot-restore/#take-snapshots (https://opensearch.org/docs/1.2/opensearch/snapshot-restore/#take-snapshots)

For virtual appliances, you can use industry best practices defined for VMware or Windows Hyper-V.

Note: Although there are no registered cases with third-party agents interfering with CYBERQUEST's processes, it is recommended to use an agentless tool for backing up virtual appliances. Many tools on the market, like VEEAM or Quest Rapid Recovery, use an agent installed on hypervisor to handle virtual machines, therefore installing nothing on the virtual machine itself. However, if you need to deploy a backup agent within the virtual appliance, please address Nextgen Software support team for any issues with platform's native processes.

Default backup locations for 3rd party backup solutions are:

a. Configuration database settings Default: **/data/mysqlbackups/folder**

b. Event data backup Default: **/data/storage/default/folder**

c. The current CYBERQUEST/CYBERQUEST installation files: Default: **/var/opt/Cyberquest/folder**

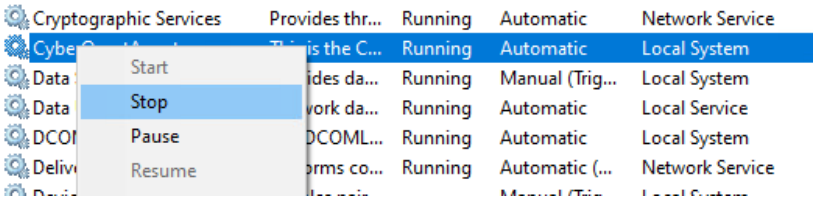
Disaster Recovery

How to create Backups

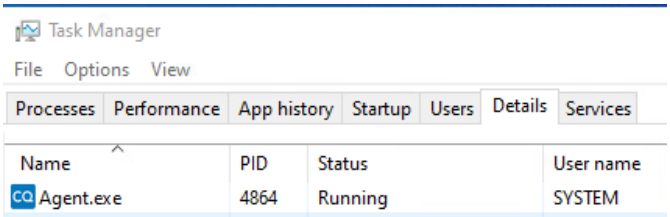
1.Backup CYBERQUEST Agent

In the event of a disaster, to save the Agent's configurations and data sources, please follow these steps:

A. On the Windows machine where the CYBERQUEST Agent is installed, open Windows Services and **stop** the CYBERQUEST Agent service.



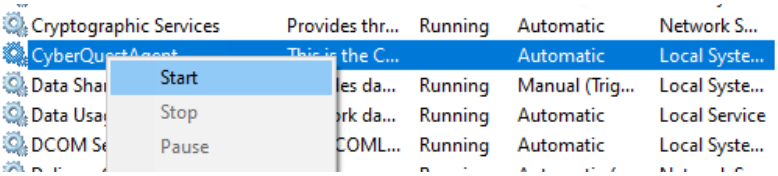
To check if the CYBERQUEST Agent has stopped, open **Task Manager > Details** and wait until the **Agent.exe** process disappears from Task Manager.



B. Copy the folder **datasources** to another machine. The folder is in the following path:

```
C:\Program Files\CyberQuestAgent\datasources
```

C. Open Windows Services and **start** the CYBERQUEST Agent service.



To verify that the CYBERQUEST Agent has started, open **Task Manager> Details** and wait until the **Agent.exe** process appears in the Task Manager.

2.Backing up configuration server side

To back up configurations, we need to export the two databases, config and reports.

Config contains CYBERQUEST application settings such as alert settings, jobs, dictionaries, and CYBERQUEST service settings.

Reports contains CYBERQUEST application customizations at dashboards, dashgroups, reports, agents and users.

To back up the two databases, we need to follow these steps:

A.Authenticate in CYBERQUEST server via ssh

B.Change the path using the following command:

```
cd /home/superadmin/
```

C.Create the folder **bkp** where the data will be saved:

```
mkdir  bkp
```

D.Change the path to the newly created folder:

```
cd bkp
```

E.Use the following commands to back up the two databases:

```
mysqldump -u root -p --databases reports > reports.sql
```

```
mysqldump -u root -p --databases config > config.sql
```

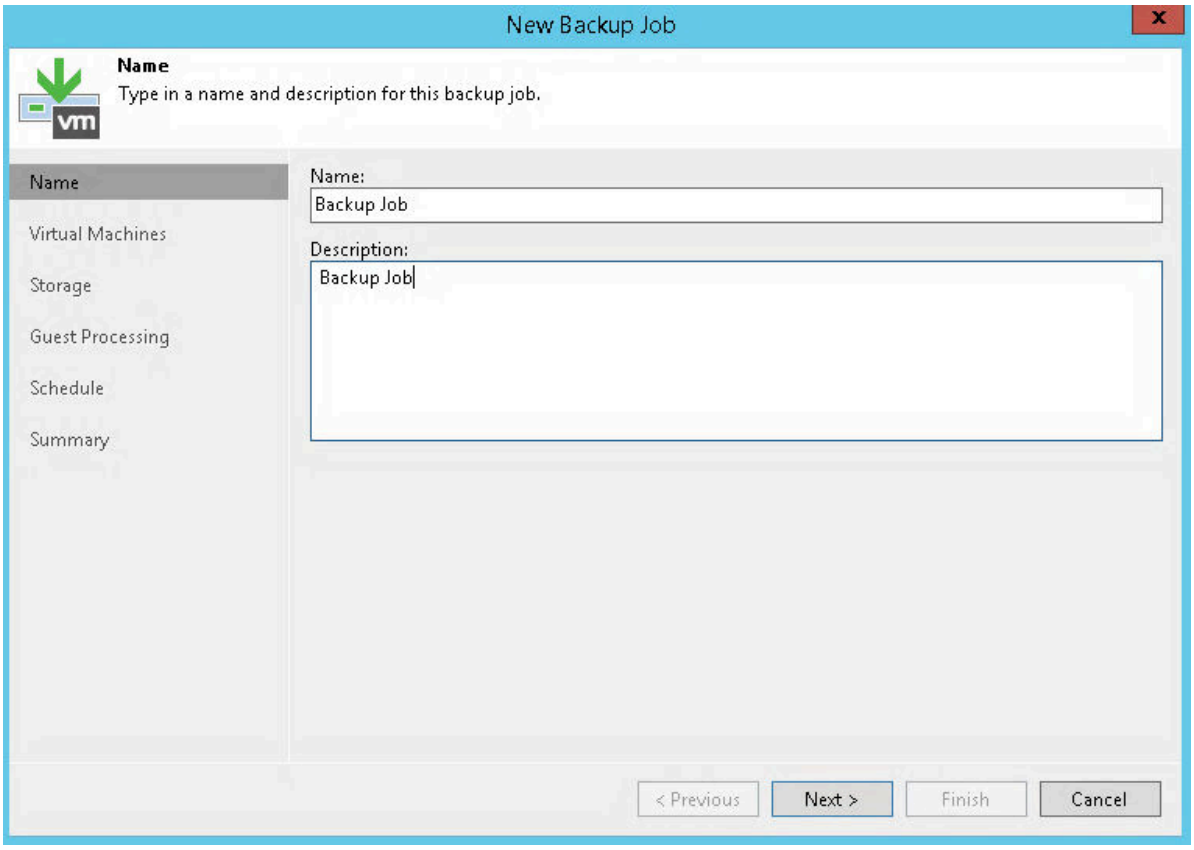
F.Copy the **bkp** folder to another machine to complete the backup process.

3.Backup Virtual Appliance

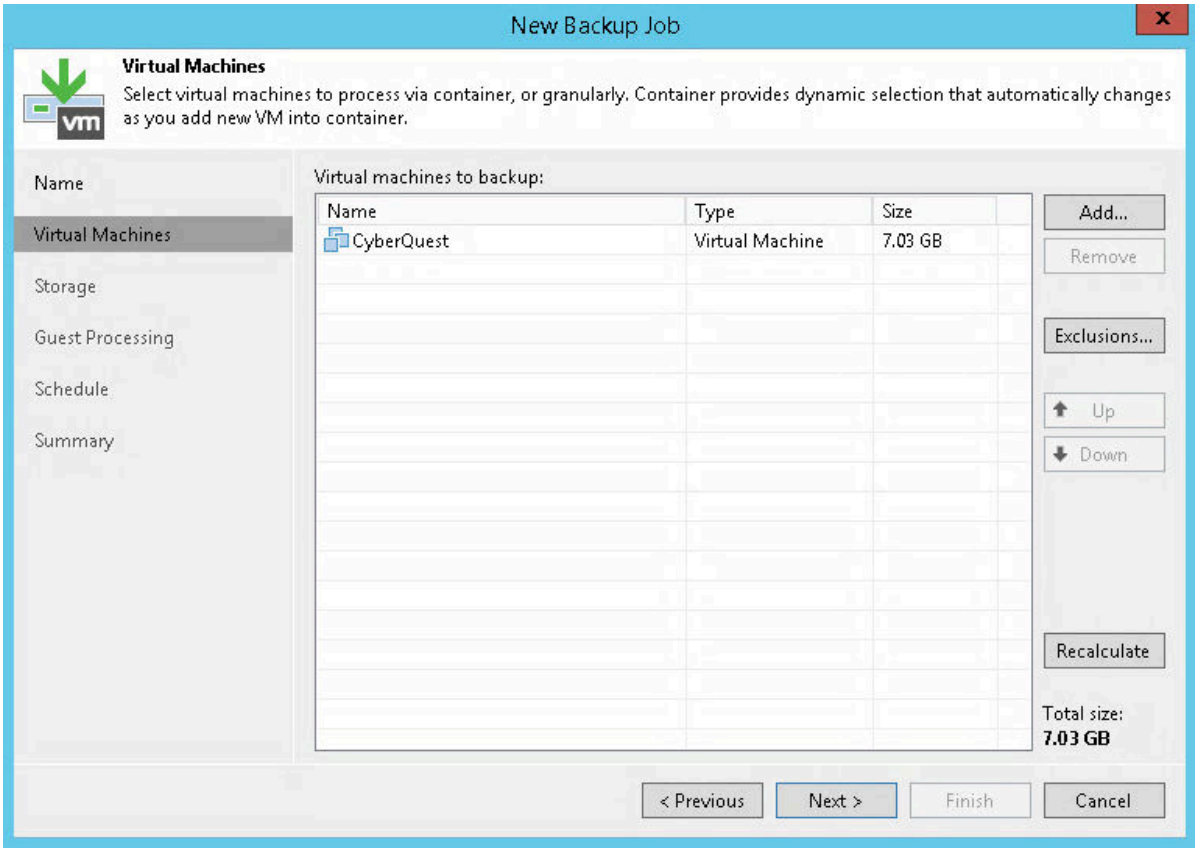
It is recommended to use a tool for backing up virtual appliances. Many tools on the market, like VEEAM or Quest Rapid Recovery, use an agent installed on hypervisor to handle virtual machines, therefore installing nothing on the virtual machine itself.

A.Open Veeam application

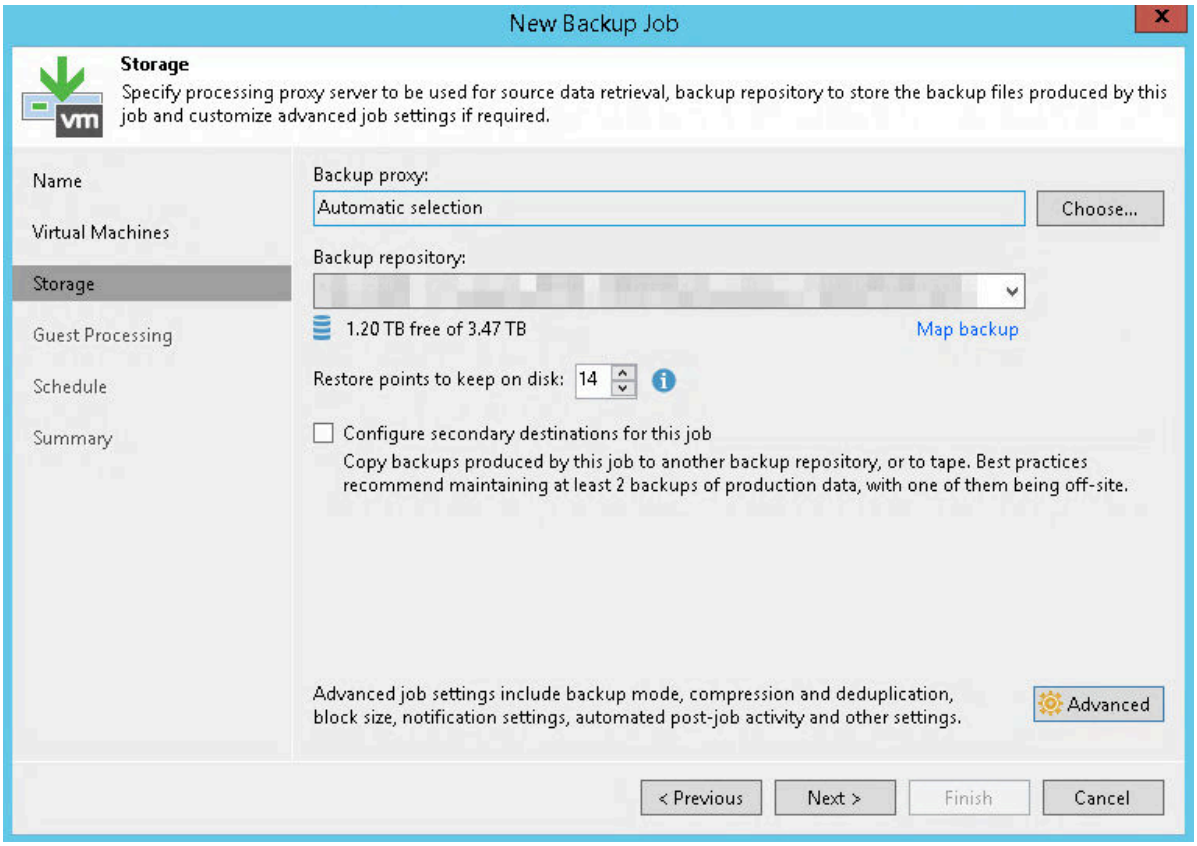
B.Create a Backup Job. Add name and description



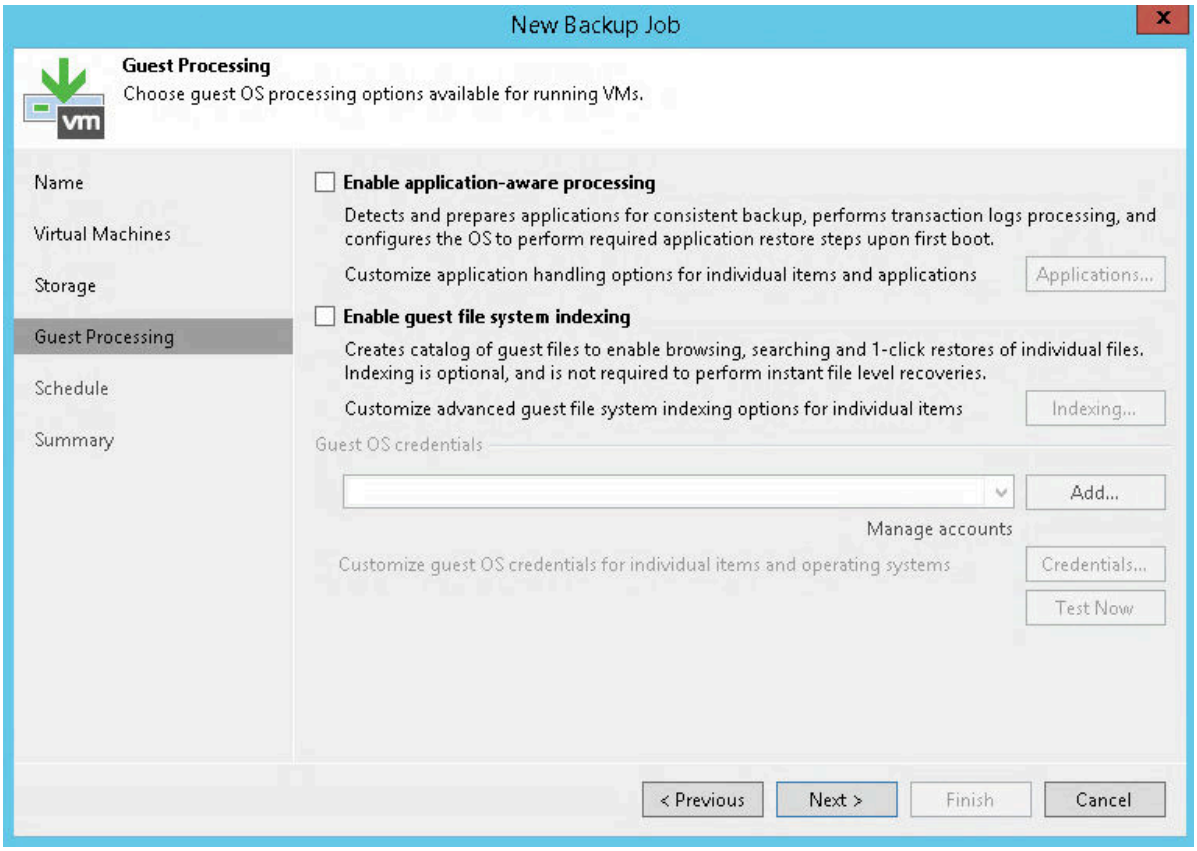
C.Select Virtual Machine to backup data



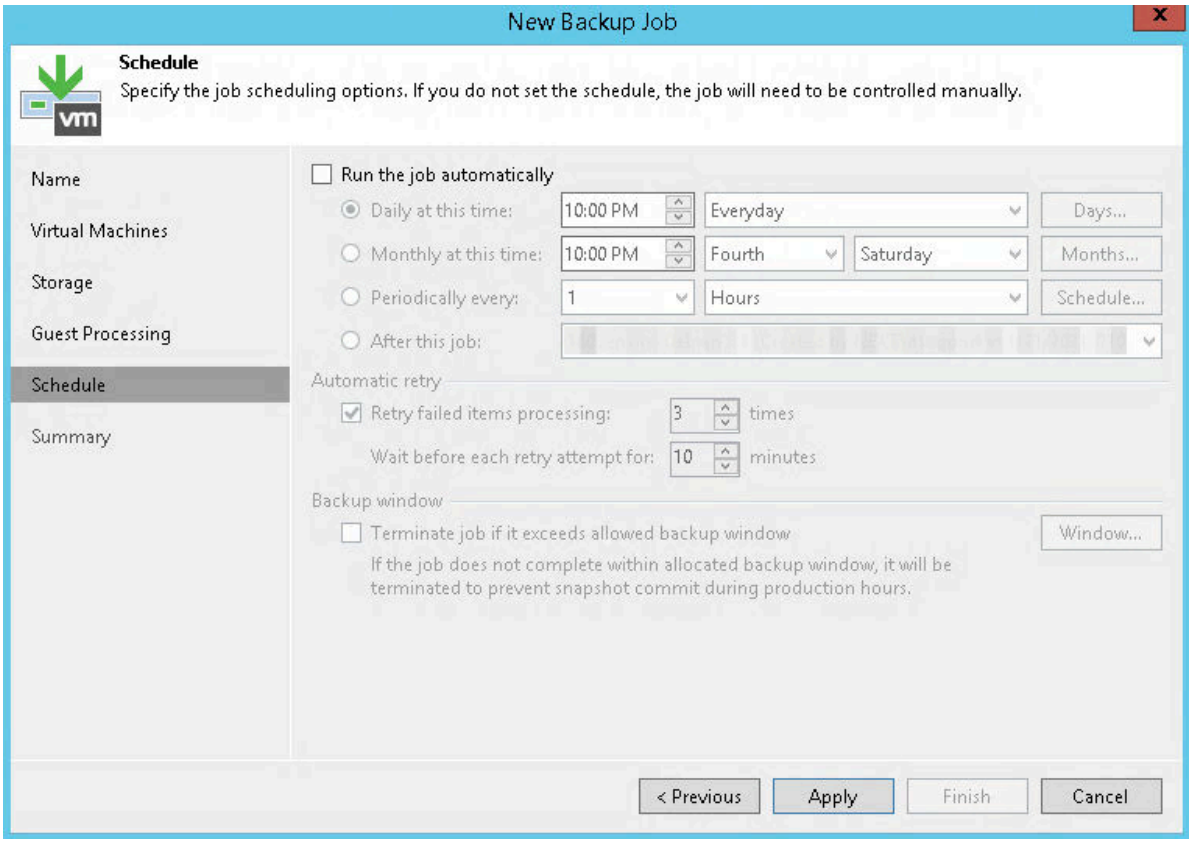
D.Select backup repository to save data and number of restore days



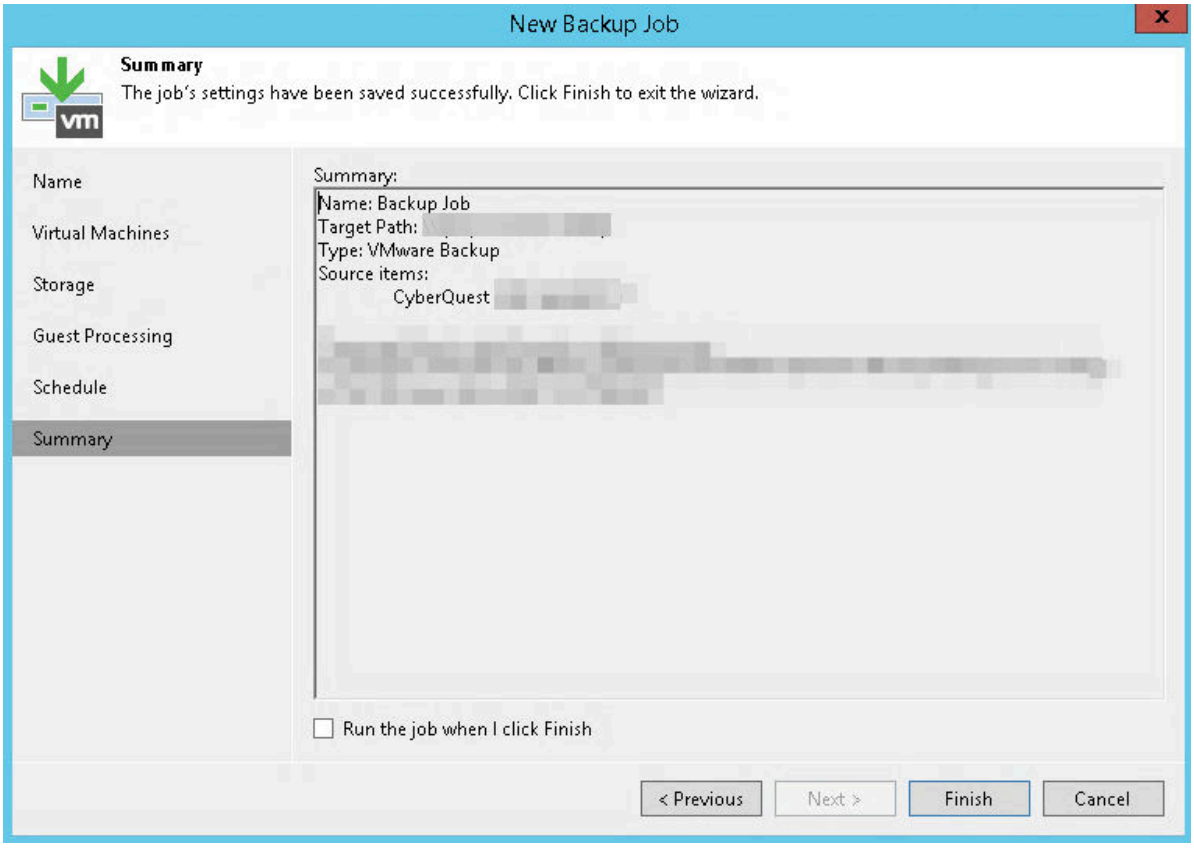
E.Choose guest OS processing options



E.Schedule the execution job

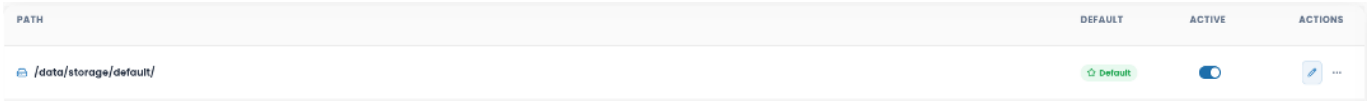


F. Summary



4.Backup data storage data

Every message collected by CYBERQUEST is automatically sent to data storages, as configured in **Settings > Data Storages** page:



Stored events are normalized in JSON format, compressed, encrypted and digitally signed. They can be later imported to a backup storage.

The default path is: **/data/storage/default**

The **default** folder must be copied to another external storage medium (outside CYBERQUEST).

5.Backup Online DataStorage data

Every message collected by CYBERQUEST is automatically sent to short term storage (Online DataStorage).

The default path is: **/data/opensearch**

The **Online DataStorage** folder must be copied to another external medium (outside CYBERQUEST).

CQ EventIDs

CYBERQUEST EventIDs

EventID	Event Name	Description	Scope
9170001	WindowsPerformance Meters CPU Mem Event	Generates an event reporting the percentage usage of CPU and RAM, including detailed system metrics over time	Monitor overall Windows system performance, detect abnormal CPU or memory spikes, and support proactive resource management
9170002	WindowsPerformance Meters Logical Drive Event	Generates an event reporting the utilization percentage of a specific logical drive, including space consumed and remaining	Track disk usage trends, identify potential storage bottlenecks, and alert before resource exhaustion on Windows systems
9175001	DataAcquisitionMetering Event	Captures detailed resource and performance metrics of the system where Data Acquisition CQ is installed	Monitor host-level resource consumption, identify performance issues impacting data acquisition processes, and ensure system stability
56789	Self Audit	Reports audit activities from the CQ Web Application, including user actions and system changes	Enable monitoring and compliance tracking for web application usage, detect unauthorized access, and support security audits
580466301	An object was moved from *SourceFile* to *Destination*	Logs files that have been moved, including original and new paths	To identify, in Microsoft Windows environments, the moved files with the location before and after the move.
580466302	An object was deleted	Logs deleted files, including file name, path, and deletion timestamp	Identify and investigate deleted files or objects, supporting forensic analysis and detection of potential malicious activity
580466303	A new file was createad or modified	Logs newly created or modified files, including file name and full path	Monitor creation and modification of files to detect unauthorized changes or suspicious activity in Windows systems
580466304	A new folder was created	Logs newly created folders with full paths	Detect creation of new directories, monitor organizational changes, and flag unexpected folder activity for investigation
580466305	An object was renamed *SourceFile* to *DestinationFile*	Logs files or folders that have been renamed, including previous and new names and paths	Track renaming of files and folders to detect suspicious or unauthorized changes in Windows environments
580466306	An object was accessed	Logs accessed files, including file name, path, and access type	Monitor file access activity to detect unauthorized or suspicious interactions with sensitive files
9160000	VPN	Generates events related to VPN activity, including connection attempts, success, failure, and source geolocation	Monitor remote access activity, detect unusual login locations or devices, and support forensic investigations of VPN usage
63805	NetFlow v5	Reports detailed traffic information for IP communications, including source/destination IPs, ports, and protocol usage	Monitor network traffic patterns, detect anomalies, and support network security and performance analysis for NetFlow v5 environments
63809	NetFlow V9	Reports detailed IP traffic flows using the NetFlow v9 protocol, including advanced flow attributes	Monitor and analyze network communications, detect unusual traffic, and

EventID	Event Name	Description	Scope
			support threat detection and network optimization
63810	IPFIX or NetFlow V10	Reports IP traffic using IPFIX or NetFlow v10, including enhanced metadata and flow statistics	Enable advanced monitoring of network traffic, correlate flows for security events, and support high-fidelity network analysis
63900	BiFlow Events	Reports bidirectional traffic between IPs, combining source and destination flows for context	Detect abnormal bidirectional communications, monitor application-level traffic patterns, and support threat correlation
9150001	Windows Success Interactive Logon Activity	Logs successful interactive user logins, including user identity, workstation, and login timestamp	Detect new interactive logins, monitor user activity patterns, and identify unauthorized access attempts on Windows systems
9150002	Windows Success Network Logon Activity	Logs successful network logins, including username, source IP, and target system	Detect new network logins, monitor access to shared resources, and identify potential lateral movement or unauthorized network access
9150003	Windows Success Batch Logon Activity	Logs successful batch logins, such as scheduled tasks, including user and host details	Monitor automated or scheduled task logins to detect unusual or suspicious batch activities
9150004	Windows Success Service Logon Activity	Logs successful service logins, including service name, host, and source IP	Track service authentications, detect new or unexpected services starting on the network, and monitor for potential security breaches
9150005	Windows Success Network Cleartext Logon Activity	Logs successful cleartext logins across the network, including user and source IP	Detect insecure authentication events, monitor network login patterns, and flag potentially risky cleartext logins
9150006	Windows Success Remote Interactive Logon Activity	Logs remote interactive logins with user and source IP details	Detect remote access activity, identify anomalous login behavior, and support endpoint monitoring for Windows environments
9150007	Windows Success Cached Interactive Logon Activity	Logs cached interactive logins occurring after a break period of ≥3 months	Monitor long-term cached login activity, detect unusual delayed logins, and track endpoint access patterns
9150011	Windows Failed Interactive Logon Activity	Logs failed interactive login attempts with user and source IP	Detect unsuccessful login attempts, monitor for brute-force attacks, and enhance Windows access security
9150012	Windows Failed Network Logon Activity	Logs failed network login attempts including username and source IP	Identify failed network authentication attempts, detect suspicious activity, and prevent unauthorized access
9150013	Windows Failed Batch Logon Activity	Logs failed batch login attempts such as scheduled tasks	Detect automation failures or malicious batch login attempts in Windows systems
9150014	Windows Failed Service Logon Activity	Logs failed service authentication attempts	Identify service login failures, detect misconfigurations, and prevent potential security breaches
9150015	Windows Failed Network Cleartext Logon Activity	Logs failed cleartext network logins	Detect failed cleartext authentication attempts
9150016	Windows Failed Remote Interactive Logon Activity	Reports failed remote interactive logins	Detect failed remote logins in Windows environments
9150017	Windows Failed Cached Interactive Logon Activity	Reports failed cached interactive logins after ≥3 months	Monitor failed long-term cached logins

EventID	Event Name	Description	Scope
9150051	Windows Success Service Activity Service	Reports network machine logins and newly registered services	Detect new network service authentications
9150052	Windows Success Service Activity Service User	Reports newly registered service/user combinations	Track new service logins under specific users
9150053	Windows Success Service Activity Service Computer	Reports service logins on network machines	Track new services running on network machines
9150061	Windows Failed Service Activity Service	Reports failed authentications for new services	Detect failed service logins
9150062	Windows Failed Service Activity Service User	Reports failed service/user login combinations	Monitor failed service logins under users
9150063	Windows Failed Service Activity Service Computer	Reports failed service logins on network machines	Monitor failed service logins on computers
9150101	Linux Success Sshd Logon Activity	Reports SSH logins with user and host	Detect new SSH logins in Linux environments
9150102	Linux Success Sudo Logon Activity	Reports SUDO logins with user and host	Detect new SUDO logins in Linux environments
9150103	Linux Success Su Logon Activity	Reports SU logins with user and host	Detect new SU logins in Linux environments
9150104	Linux Success Systemd Logon Activity	Reports logins via Systemd with user and source IP	Detect new Systemd logins in Linux environments
9150151	Linux Failed Logon Activity SSH	Reports failed SSH logins with user and host	Detect failed SSH logins in Linux environments
9150201	VPN Success Logon Activity by Country	Reports successful VPN logins with user and country	Monitor new username/geolocation combinations
9150202	VPN Success Logon Activity by ClientIP	Reports successful VPN logins with user and IP	Monitor new username/IP combinations

How-to · AD information needed to read AD objects

To collect attributes information of Active Directory objects, please follow instructions below:

- Read access credentials for Active Directory Objects

Attributes of Active Directory are:

- password never expires attribute
- account status
- lost logon
- bad logon count
- last bad password attempt
- department
- title
- and so on

How-to · Collecting Mysql-data

Collecting Mysql-data in CYBERQUEST

This guide describes the procedure for audit activation on MariaDB.

1.In order to activate the audit on MariaDB, perform the following actions:

A.Open mysql config file using the following command:

```
nano /etc/mysql/my.cnf
```

B.Add the following lines [mysqld]:

```
plugin_load=server_audit=server_audit.so
server_audit_events=connect,query,table
server_audit=FORCE_PLUS_PERMANENT
```

C.Restart mysql service with the following command:

```
systemctl restart mysql.service
```

The default location for the logs is : **/var/lib/mysql/server_audit.log**

2.If syslog logging is required follow the steps from bellow:

A.Open mysql config file using the following command:

```
nano /etc/mysql/my.cnf
```

B.Add the following parameter:

```
server_audit_output_type=SYSLOG
```

C.Restart mysql service with command:

```
systemctl restart mysql.service
```

Check parameters with the following command:

```
SHOW GLOBAL VARIABLES LIKE 'server_audit%';
```

Check syslog logging with the following command:

```
tail -f /var/log/syslog OR tail -f /var/log/messages
```

Reference:

https://mariadb.com/kb/en/library/mariadb-audit-plugin-installation/ (https://mariadb.com/kb/en/library/mariadb-audit-plugin-installation/)

How-to · How to collect in a table from a PostgreSQL database

To collect log events from a PostgreSQL database audit table, the following prerequisits must be met:

- The user has permission to read the audit table;
- Having Server IP and port;
- Having an audit table structure, including Database name and table name;
- Editing the sql query as follows, using the table structure chosen:

```
select

to_char(&amp;quot;TimestampColumn&amp;quot;,'YYYY-MM-DD HH24:MI:SS.US') as LocalTime,

&amp;quot;Column1&amp;quot;,

&amp;quot;Column2&amp;quot;,

&amp;quot;Column3&amp;quot;,

&amp;quot;Column4&amp;quot;,

&amp;quot;Column5&amp;quot;,

&amp;quot;Column6&amp;quot;,

&amp;quot;Column7&amp;quot;,

&amp;quot;Column8&amp;quot;,

&amp;quot;Column9&amp;quot;,

&amp;quot;Column10&amp;quot;

from DataBaseName.&amp;quot;AuditTableName&amp;quot;

where &amp;quot;TimestampColumn&amp;quot; > TO_TIMESTAMP('$LastDateTime$', 'YYYY/MM/DD HH24:MI:SS.US')

order by &amp;quot;TimestampColumn&amp;quot;
```

How-to · How to collect logs from AWS CloudFront

To collect log events from a AWS CloudFront, the following prerequisits must be met:

- Export the logs from AWS CloudFront into a monitoring folder;
- Access to the custom file script processing template provided with the CYBERQUEST Windows agent, found in the installation folder (go to C:\Program Files\CyberQuestAgent\templates). Use the template to process the exported files from AWS in the monitoring folder.

How-to · How to collect logs from AWS CloudTrail

To collect log events from a AWS CloudTrail, the following prerequisits must be met:

- Export the logs from AWS CloudTrail into a monitoring folder;
- Access to the custom file script processing template provided with the CYBERQUEST Windows agent, found in the installation folder (go to C:\Program Files\CyberQuestAgent\templates). Use the template to process the exported files from AWS in the monitoring folder.

How-to · How to collect logs from Squid

To collect log events from Squid, activate the logging of events at site level.

Add the following row in the Squid configuration file (which can be found at **/etc/squid/squid.conf**):

```
access_log udp://10.10.10.10:5140 squid //use this line with your own CYBERQUEST IP address
```

The example above fits Ubuntu and Debian operating systems.

How-to · How to configure Apache to send logs to CYBERQUEST server

To integrate Apache logs into CYBERQUEST, follow these steps:

1. **Log in** to the server that hosts Apache, as the root user
2. **Edit** the Apache configuration file **httpd.conf**
3. **Add** the following information in the Apache configuration file to specify the custom log format: LogFormat "%h %A %l %u %t "%r" %>s %p %b" (where is a variable name you provide to define the log format)
4. **Add** the following information in the **Apache configuration file** to specify a custom path for the syslog events:

CustomLog "|/usr/bin/logger -t httpd -p <*facility*>.<*priority*>" <*log format name*>, where:

- <*facility*> is a syslog facility (for example, local0)
- <*priority*> is a syslog priority (for example, info or notice)
- <*log format name*> is a variable name that you provide to define the custom log format and must match the log format name that is defined at **Step 3**, for example:

```
CustomLog "|/usr/bin/logger -t httpd -p local1.info" MyApacheLogs
```

5. **Type** the following command to disable *hostname* lookup: **HostnameLookups off**
6. **Save** the Apache configuration file
7. **Edit** the syslog configuration file:

```
/etc/syslog.conf
```

8. **Add** the following information to your syslog configuration file:

<*facility*>.<*priority*> <*TAB*><*TAB*>@<*host*>:5140, where:

- <*facility*> is the syslog facility (for example, local0) and must match the value that you typed in **Step 4**
- <*priority*> is the syslog priority (for example, info or notice) and must match the value that you typed in **Step 4**
- <*TAB*> indicates you must press the **Tab** key

- <*host*> is the IP address of the CYBERQUEST

9. **Save** the syslog configuration file

0. **Type** the following command to restart the syslog service:

```
/etc/init.d/syslog restart
```

11. **Restart** Apache to complete the syslog configuration

How-to · How to configure CYBERQUEST to collect MS exchange tracking logs

To collect log events from MS exchange tracking logs, the following prerequisits must be met:

- Copy the exchange tracking logs to CQ Monitored folder.
- Edit "exchangeTrackingLog1.xml" (which can be found at C:\Program Files\CyberQuestAgent\templates), and modify the following TAG:

```
<add name="monitorFolder" value="C:\\ImportedTrackingLogs\\Exchange1"/>
```

How-to · How to configure DarkTrace to send logs to CYBERQUEST server

Darktrace is a network traffic analyzing tool that delivers notification events to downstream systems. The collector can be configured to capture these notification events and generate investigations around them.

Before you begin

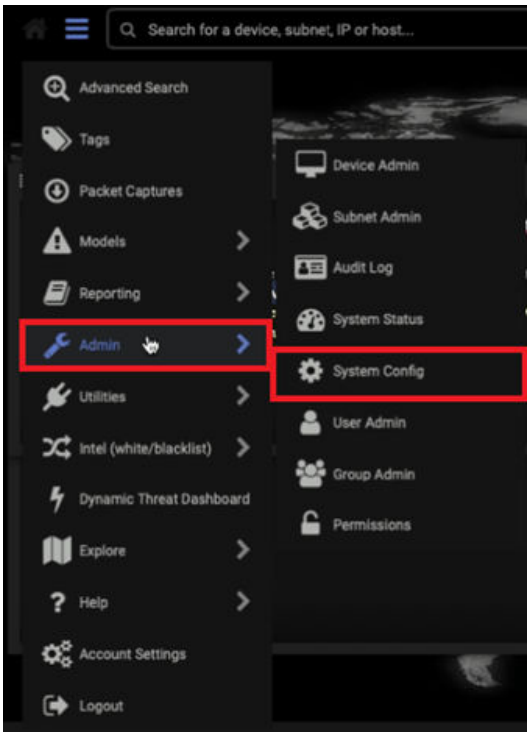
You must configure Darktrace to send syslog to the CYBERQUEST Server. You must be a Darktrace administrator with access to the user interface.

To configure syslog forwarding for Darktrace, please follow the steps bellow:

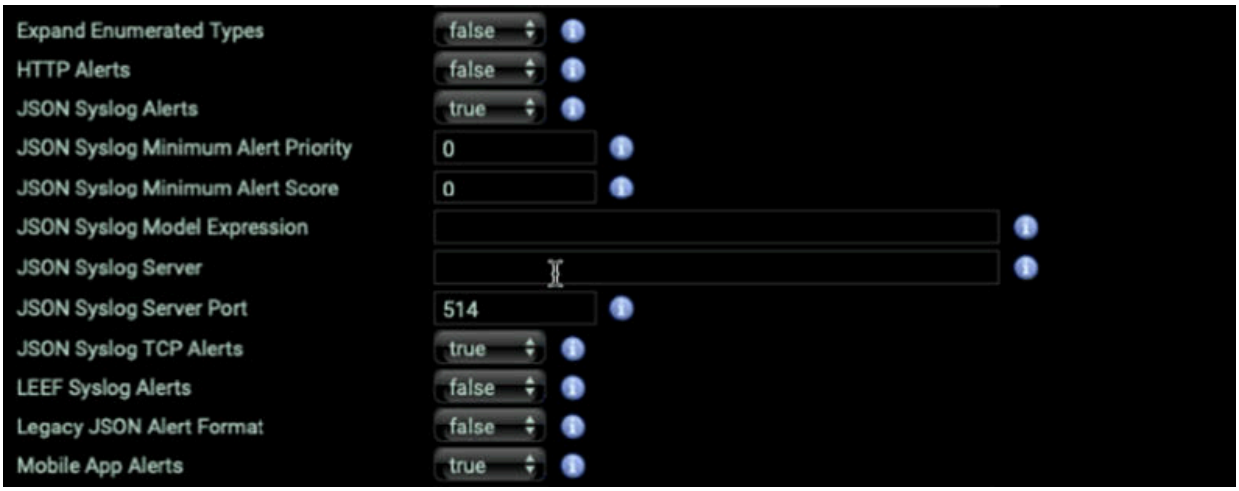
1. Log in to **Darktrace interface**

2. Expand top left menu and select *Admin*, a second menu appears

3. Select **System Config** page



4. In *Alerting* section, click on **Verify Alert Settings**
5. In *JSON Syslog Alerts*, set field to **True**
6. Set syslog server to **CYBERQUEST Server's IP address**
7. Set a **port 5140 UDP** to use with the CYBERQUEST event source
8. Set *JSON Syslog TCP Alerts* to **True**



How to Configure This Event Source

1. From your **dashboard**, select *Data Collection* on the left-hand menu
2. When *Data Collection* page appears, click on **Setup Event Source** drop-down and pick **Add Event Source**
3. From *Third Party Alerts* section, click the **Darktrace** icon
4. **Add Event Source** panel appears
5. Choose your **collector** and event **source** (you can also name your event source)
6. Optionally send unfiltered logs
7. Enter the **port** you chose in the **Darktrace interface**

8. Select **TCP** as your protocol

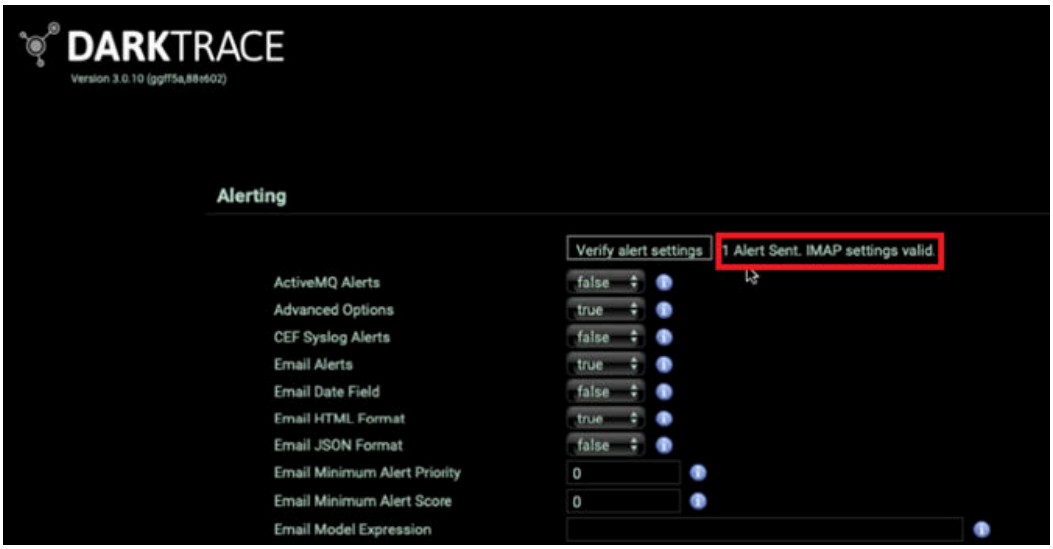
9. Click **Save**

Verify the configuration

After you configure the event source, you can send a test alert from Darktrace to verify everything is working properly.

To send a test alert, please follow the steps bellow:

1. Return to **Darktrace interface**
2. Expand top left menu and select *Admin,* a second menu appears
3. Select **System Config** page
4. In the *Alerting* section, click on **Verify Alert Settings**
5. **1 Alert Sent. IMAP settings valid** message appears



How-to · How to configure File Integrity Monitoring (FIM) on Linux servers

How to Configure File Integrity Monitoring (FIM) on Linux Servers

FIM monitors selected files for changes to their content and attributes. It helps identify unexpected changes to important system and application files. For more information about the Linux Agent and its file-system security monitoring capabilities, see Linux Agent.

What File Integrity Monitoring detects

The Linux FIM data source periodically compares monitored files with their previously recorded signatures, including content hash, size, last modification time, permissions, attributes, and ownership. Depending on the change, it can generate events for:

- **File created**: A file appears in a monitored location.
- **File modified**: File content or tracked attributes change.
- **File deleted**: A previously monitored file is removed.

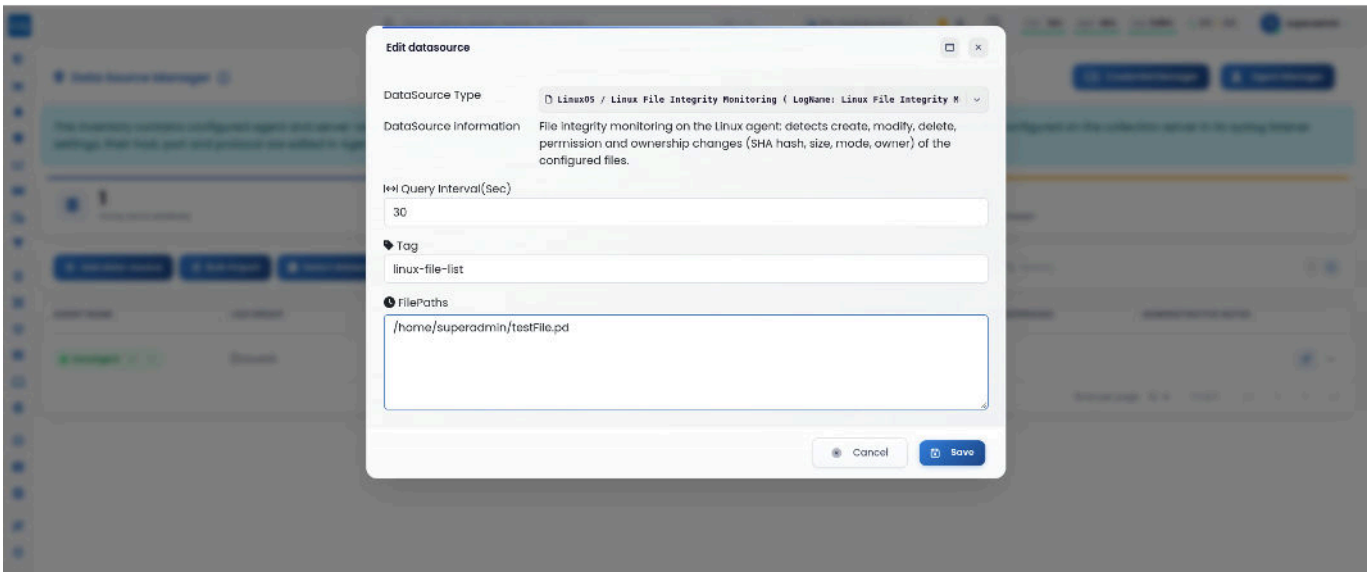
Prerequisites

- A Linux server with the CYBERQUEST Linux Agent installed and communicating with CYBERQUEST.
- Administrative permissions to configure data sources in the CYBERQUEST web interface.
- Read permissions for the agent on the selected files and directories.

Configure the Linux File Integrity Monitoring data source

Log in to the CYBERQUEST web interface and navigate to **Settings > Management > Data Source Manager**.

Add or locate the **LinuxOS / Linux File Integrity Monitoring** data source and assign it to the Linux Agent on the monitored server. Confirm that the agent is assigned in the data source list.



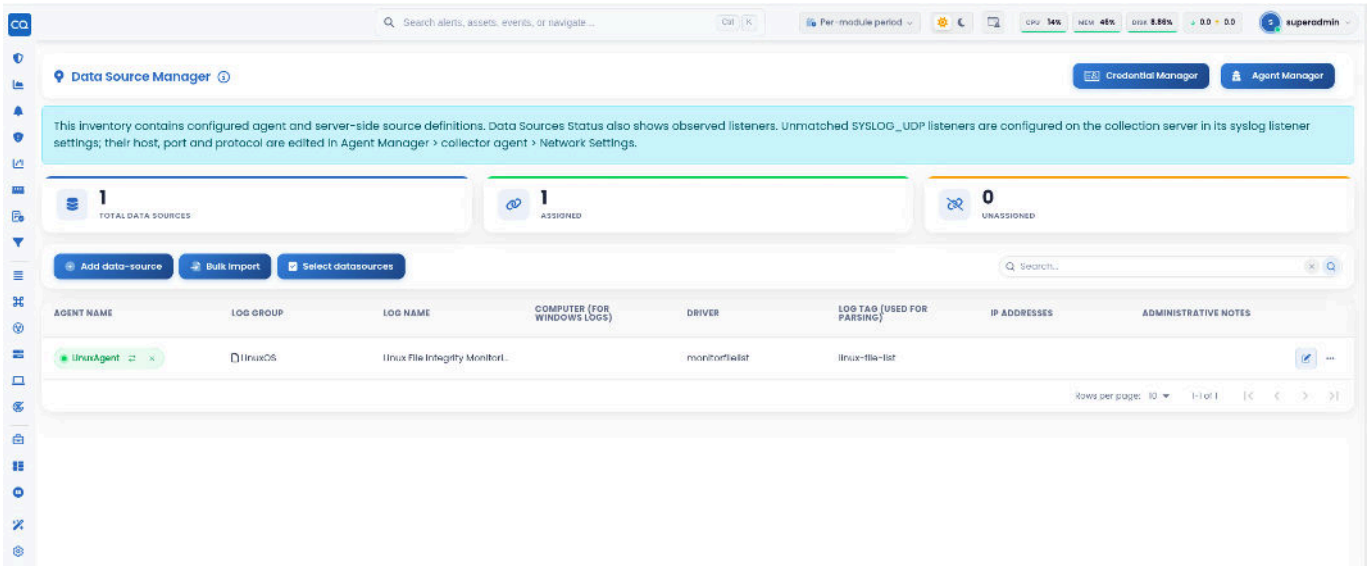
Configure these parameters:

- **DataSource Type** - Select LinuxOS / Linux File Integrity Monitoring.
- **Query Interval (Sec)** - Interval between file checks; the example configuration uses 30 seconds.
- **Tag** - Tag used to identify events in CYBERQUEST; for example, linux-file-list.
- **FilePaths** - Full paths of files to monitor, with one entry per line.

In the illustrated configuration, **FilePaths** contains /home/superadmin/testFile.pd.

Select **Save** to apply the settings.

Linux File Integrity Monitoring data source assigned to the Linux Agent.



Monitor individual files or groups of files

To monitor individual files, enter their absolute paths, one per line:

```
/etc/passwd
/etc/ssh/sshd_config
```

To monitor multiple files under a directory, use a regex: entry. The syntax is:

```
<root-directory>/regex:<.NET-regular-expression>
```

For example:

```
/etc/nginx/regex:\.conf$
/home/superadmin/testFolder/regex:.*
```

The first expression matches .conf file names under /etc/nginx; the second matches files under the chosen test directory. These expressions are evaluated recursively, including subdirectories.

Verify File Integrity Monitoring events

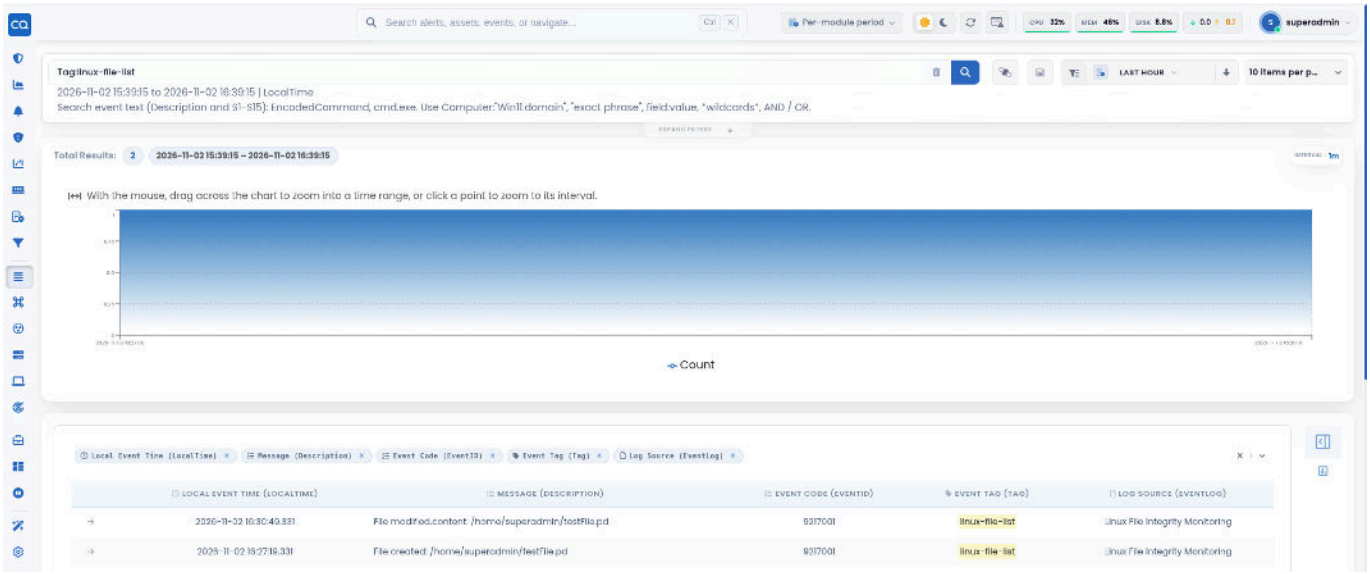
For a safe validation, monitor a disposable test file rather than modifying an important operating system file. For example, on the monitored Linux server, create a dedicated test file and modify its contents:

```
mkdir -p /tmp/cq-fim-test
printf 'initial content\n' > /tmp/cq-fim-test/test.txt
printf 'updated content\n' >> /tmp/cq-fim-test/test.txt
```

Before running this example, configure **FilePaths** to include */tmp/cq-fim-test/test.txt*. Allow at least one monitoring interval between baseline creation and the modification if you want separate events for each step. This command sequence is a suggested validation procedure; the screenshots below show results from a separate test file.

In CYBERQUEST, open **Browser** and search using the configured tag:

```
Tag:linux-file-list
```



Review the event timestamp, description, EventID, tag, and log source. The following screenshot shows two FIM events associated with the monitored file: File created and **File modified.content**. File creation and content modification events in CYBERQUEST Browser. In the demonstrated results, the events have EventID 9217001 and are identified by the log source

How-to · How to configure Firewall CheckPoint to send logs to CQ Server IP Address on port 5140 UDP

Configuring System Logging - Gaia Portal

This section includes procedures for configuring System Logging and Remote System Logging

System Logging configures if Gaia sends these logs:

- Gaia syslog messages to its Check Point Management Server
- Gaia audit logs upon successful configuration to its Check Point Management Server
- Gaia audit logs upon successful configuration to Gaia syslog facility

Remote System Logging configures a remote syslog server, to which Gaia sends its syslog messages (there are some command options and parameters, which you cannot configure in the Gaia Portal)

To configure System Logging, please follow the steps bellow:

1. In the navigation tree, click **System Management > System Logging**.
2. In the **System Logging** section, select the applicable options:

- Send Syslog messages to management server
- Specifies if the Gaia sends the Gaia system logs to a Check Point Management Server. **Default: Not selected** (this option is configured in the Gaia Clish with the set syslog cplogs {on | off} command)
- Send audit logs to management server upon successful configuration
- Specifies if the Gaia sends the Gaia audit logs (for configuration changes that authorized users make) to a Check Point Management Server. **Default: Selected** (this option is configured in the Gaia Clish with the set syslog mgmtauditlogs {on | off} command)
- Send audit logs to syslog upon successful configuration
- Specifies if the Gaia saves the logs for configuration changes that authorized users make. **Default: Selected**
- To specify a desired Gaia configuration audit log file, run the set syslog filename <*/Path/File*> command, otherwise Gaia uses the default /var/log/messages file (this option is configured in the Gaia Clish with the set syslog auditlog {disable|permanent} command)

3. Click **Apply**

To configure Remote System Logging, please follow the steps bellow:

1. In the navigation tree, click **System Management > System Logging**
2. In the **Remote System Logging** section, click **Add**
3. In the **IP Address** field, enter I**Pv4 address** of the remote syslog server
4. In the **Priority** field, select **severity level** of logs that are sent to remote server. These are the accepted values:
    - **All** - All messages
    - **Debug** - Debug-level messages
    - **Info** - Informational messages
    - **Notice** - Normal but significant condition
    - **Warning** - Warning conditions

- **Error** - Error conditions
- **Critical** - Critical conditions
- **Alert** - Action must be taken immediately
- **Emergency** - System is unusable

5. Click **OK**

To edit Remote System Logging settings, please follow the steps bellow:

1. In the navigation tree, click **System Management > System Logging**
2. In the **Remote System Logging** section, select the remote server
3. Click **Edit**
4. In the **IP Address** field, enter **IPv4 address** of the remote syslog server
5. In the **Priority** field, select **severity level** of logs that are sent to remote server
6. Click **OK**

To delete Remote System Logging settings, please follow the steps bellow:

1. In the navigation tree, click **System Management > System Logging**
2. In the **Remote System Logging** section, select the remote syslog server
3. Click **Delete**
4. Click **Yes**

Syntax for System Logging configuration

To send the Gaia system logs to a Check Point Management Server:

```
set syslog cplogs {on | off}
```

To send the Gaia configuration audit logs to a Check Point Management Server:

```
set syslog mgmtauditlogs {on | off}
```

To save the Gaia configuration audit logs:

```
set syslog auditlog {disable | permanent}
```

To configure the file name of the Gaia configuration audit log:

```
set syslog filename </Path/File>
```

To show the Gaia system logging configuration:

show syslog

all

auditlog

cplogs

filename

mgmtauditlogs

Note: After you add, configure, or delete features, run the **save config** command to save the settings permanently

Syntax for Remote System Logging configuration

To send Gaia system logs to a remote syslog server:

```
add syslog log-remote-address <IPv4 Address> level <Severity>
```

To show the Gaia system logging configuration:

show syslog

all

log-remote-address <IPv4 Address>

log-remote-addresses

To stop sending Gaia system logs to the specific remote server:

```
delete syslog log-remote-address <IPv4 Address> [level <Severity>]
```

Note: After you add, configure, or delete features, run the **save config** command to save the settings permanently

Parameters and descriptions

Parameters	Description
cplogs {on \ off}	Specifies if the Gaia sends the Gaia system logs to a Check Point Management Server: **on** – Send Gaia system syslogs **off** – Do not send Gaia syslogs **Default**: off **Note** – This command corresponds to the **Send Syslog messages to management server** option in the Gaia Portal > **System Management > System Logging**.
Mgmtauditlogs {on \ off}	Specifies if the Gaia sends the Gaia audit logs (for configuration changes that authorized users make) to a Check Point Management Server: **on** – Send Gaia audit logs **off** – Do not send Gaia audit logs **Default:** on **Note –** This command corresponds to the **Send audit logs to management server upon successful configuration** option in the Gaia Portal > **System Management** > **System Logging**.
Auditlog {disable \ permanent}	Specifies if the Gaia saves the logs for configuration changes that authorized users make: **disable** – Disables the Gaia audit log facility **permanent** – Enables the Gaia audit log facility to save information about all successful changes in the Gaia configuration. To specify a desired destination file, run the set syslog filename <*/Path/File*> command (otherwise, Gaia uses the default /var/log/messages file). **Default:** permanent **Note –** This command corresponds to the **Send audit logs to syslog upon successful configuration** option in the Gaia Portal > **System Management** > **System Logging**.
<*/Path/File*>	Configures the full path and file name of the system log. **Default:** /var/log/messages **Note –** Gaia Portal does not let you configure this setting.
Log-remote-address	Configures Gaia to send system logs to a remote syslog server. **Important –** Do not configure two Gaia computers to send system logs to each other – directly, or indirectly. Such configuration creates a syslog forwarding loop, which causes all syslog messages to repeat indefinitely on both Gaia computers. **Note –** This command corresponds to the Gaia Portal > **System Management** > **Remote System Logging**.
<*Ipv4 Address*>	Ipv4 address of the remote syslog server, to which Gaia sends its system logs. **Range:** Dotted-quad ([0-255].[0-255].[0-255].[0-255]) **Default:** No default value
<*Severity*>	Syslog severity level for the system logging. These are the accepted values (as defined by the RFC 5424 – Section-6.2.1): **emerg** – System is unusable **alert** – Action must be taken immediately **crit** – Critical conditions **err** – Error conditions **warning** - Warning conditions **notice** - Normal but significant condition **info** - Informational messages **debug** - Debug-level messages **all** - All messages **Notes:** Until you configure at least one severity level for a given remote server, Gaia does not send syslog messages. If you specify multiple severities, the most general least severe severity always takes precedence.

Examples of CheckPoint Gaia:

gaia> set syslog auditlog permanent

gaia> set syslog filename /var/log/system_logs.txt

gaia> set syslog mgmtauditlogs on

gaia> set syslog cplogs on

gaia> set syslog log-remote-address 192.168.2.1 level all

gaia> show syslog all

Syslog Parameters:

Remote Address 192.168.2.1

Levels all

Auditlog permanent

Destination Log Filename /var/log/system_logs.txt

gaia>

gaia>show syslog auditlog

permanent

gaia>

gaia> show syslog cplogs

Sending syslog syslogs to Check Point's logs is enabled

gaia>

gaia> show syslog mgmtauditlogs

Sending audit logs to Management Server is enabled

gaia>

gaia> show syslog filename

/var/log/system_logs.txt

gaia>

Configuring Log Volume - Expert Mode

On condition that there is enough available disk space, you can enlarge the log partition.

Use the **lvm_manager** tool from Expert mode:

1. Connect to the Gaia system over console
2. Reboot the Gaia system
3. During boot, press any key to enter the Boot menu (you have approximately 5 seconds)
4. Select Start in maintenance mode
5. Enter the Expert mode password
6. Use the interactive lvm_manager tool as described in the sk95566: [Expert@HostName:0]# lvm_manager

Note: Disk space is added to the log volume by subtracting it from the disk space used to store backup images

Redirecting RouteD System Logging Messages

By default, Gaia writes the RouteD syslog messages (for example, OSPF or BGP errors) to the /var/log/messages file. You can configure Gaia to write the RouteD syslog messages to the /var/log/routed_messages file instead.

To configure the redirection in the Gaia Portal, please follow the steps bellow:

1. In the navigation tree, click **Advanced Routing > Routing Options**
2. In the **Routing Process Message Logging Options** section, select **Log Routed Separately**
3. In the **Maximum File Size** field, enter the size (in **megabytes**) for each log file (default is 1 MB)
4. In the **Maximum Number of Files** field, enter the maximal number of log files to keep as default is 10 log files (/var/log/routed_messages, /var/log/routed_messages.0, /var/log/routed_messages.1, ..., /var/log/routed_messages.9)
5. Click **Apply**

To configure the redirection in the Gaia Clish, please follow the steps bellow:

1. Connect to the command line on Gaia
2. Log in to Gaia Clish
3. Run these commands:

```
HostName> set routedsyslog on
```

```
HostName> set routedsyslog size <Number of MB between 1 and 2047>
```

```
HostName> set routedsyslog maxnum \\Number of Files between 1 and 4294967295
```

```
HostName> save config
```

How-to · How to configure FortiGate to send logs to CQ Server IP Address on port 5140 UDP

A remote syslog server is a system provisioned specifically to collect logs for long term storage and analysis with preferred analytic tools.

Before you begin you must have read-write permission for Log & Report settings.

To configure syslog settings, please follow the steps bellow:

1. Go to **Log & Report > Log Setting**
2. Click the **Syslog Server** tab
3. Click **Add to display** the configuration editor
4. Complete the configuration as described in below table

Settings	Guidelines
Status	Select to enable the configuration.
Address	IP address of the CYBERQUEST server
Port	Listening port number of the syslog server. Usually this is UDP port 5140
Log Level	Select the lowest severity to log from the following choices: **Emergency**—The system has become unstable. **Alert**—Immediate action is required. **Critical**—Functionality is affected. **Error**—An error condition exists and functionality could be affected. **Warning**—Functionality might be affected. **Notification**—Information about normal events. **Information**—General information about system operations. **Debug**—Detailed information about the system that can be used to troubleshoot unexpected behavior. For example, if you select **Error**, the system sends the syslog server logs with level Error, Critical, Alert, and Emergency. If you select **Alert**, the system collects logs with level Alert and Emergency.
CSV	Send logs in CSV format. Do not use with FortiAnalyzer.
Facility	Identifier that is not used by any other device on your network when sending logs to FortiAnalyzer/syslog.
Event	Select to enable logging for events.
Event Category	Select the types of events to send to the syslog server: **Configuration**—Configuration changes. **Admin**—Administrator actions. **System**—System operations, warnings, and errors. **User**—Authentication results logs. **Health Check**—Health check results and client certificate validation check results. **SLB**—Notifications, such as connection limit reached. **LLB**—Notifications, such as bandwidth thresholds reached. **GLB**—Notifications, such as the status of associated local SLB and virtual servers. **Firewall**—Notifications for the “firewall” module, such as SNAT source IP pool is using all of its addresses.
Traffic	Select to enable logging for traffic processed by the load balancing modules.
Traffic Category	**SLB**—Server Load Balancing traffic logs related to sessions and throughput. **GLB**—Global Load Balancing traffic logs related to DNS requests.
Attack Logging	Select to enable logging for traffic processed by the security modules.
Security Category	**DoS**—SYN flood protection logs. **IP Reputation**—IP Reputation logs. **WAF**—WAF logs. **Geo**—Geo IP blocking logs.

5. **Save** the configuration

How-to · How to configure GravityZone to send logs to CQ Server IP Address on port 5140 UDP

Follow these steps to configure Bitdefender Gravityzone (On premise) to send logs to CYBERQUEST:

- Log in into GravityZone
- Click on **Configuration** > **Miscellaneous**
- Put the flag on **Enable Syslog** and write the IP of CYBERQUEST
- Click on configuration button (the rowel) in the top-right corner
- Define the events you want to send to CYBERQUEST

How-to · How to configure IPS FireEye to send logs to CQ Server IP Address on port 5140 UDP

To configure IPS FireEye to send logs to CYBERQUEST Server, please follow the below steps:

1. **Login** to FireEye NX Web UI with an admin account.
2. Navigate to **Settings > Notifications**.
3. Click **rsyslog** and check the **Event type** check box.
4. Make sure **Rsyslog** settings are:
   - Default format: CEF
   - Default delivery: Per event
   - Default send as: Alert
5. Next to the **Add Rsyslog Server** button, type **CYBERQUEST**. And, click on **Add Rsyslog Server** button.
6. Enter the **CYBERQUEST server IP** address in the **IP Address** field. (Public IP, if hosted in cloud)
7. **Check off** the Enabled check box.
8. Select **Per Event** in the **Delivery** drop-down list.
9. Select **All Events** from the **Notifications** drop-down list.
0. Select **CEF** as the **Format** drop-down list.
11. Select **UDP** from the **Protocol** drop-down list. (Default port is 5140)
12. Now, click **Update**. And click the **Test-Fire** button to send the test events to CYBERQUEST server.

How-to · How to configure Linux server to read custom log files with rsyslog

To read custom log files with rsyslog from Linux server, the following prerequisits must be met:

1.Login as **root** on the linux server

2.Edit the file ***/etc/rsyslog.conf*** (ex: nano /etc/rsyslog.conf), and add to the body the following lines:

Module (*imfile*) that enables rsyslog to convert any standard text file into a syslog message.

```
$ModLoad imfile
```

```
$InputFileName        /path/to/file
$InputFileTag         tag:
$InputFileStateFile   /path/to/state/file
$InputFileSeverity    severity
$InputFileFacility    facility
$InputRunFileMonitor
```

The settings that are required to specify an input textfile:

- replace ***/path/to/file*** with a file that you want to be monitored;
- replace ***tag:*** with the tag name for the message. You can make a parsing rule based on this tag in CYBERQUEST web interface (the tag will be preceded by ***"CQ"*** prefix)
- replace *** /path/to/state/file*** with a unique name for the state file. Make sure that you specify a name that does not already exist.
- the syslog ***severity*** to be assigned to lines read. Can be specified in textual form (e.g. "info", "warning", "error",...). By default is "notice".
- the syslog ***facility*** to be assigned to lines read. Can be specified in textual form (e.g. local0 – local7). By default is local0.
- "***$InputRunFileMonitor***" - this activates the current monitor. It has no parameters and if you forget this directive, the text file will be ignored.

3.Restarting **rsyslog**

```
systemctl restart rsyslog.service
```

How-to · How to configure Linux server to send logs to CQ Server IP Address on port 5140 UDP

To send log events from Linux server, the following prerequisits must be met:

1. Login as **root** on the linux server
2. Edit the file ***/etc/rsyslog.conf*** (ex: nano /etc/rsyslog.conf), and add at the end of the file the following line:

```
auth,authpriv.* @CQ_IP_Addres:5140
```

How-to · How to configure NetGear AP to send logs to CQ Server IP Address on port 5140 UDP

Configure Log Settings

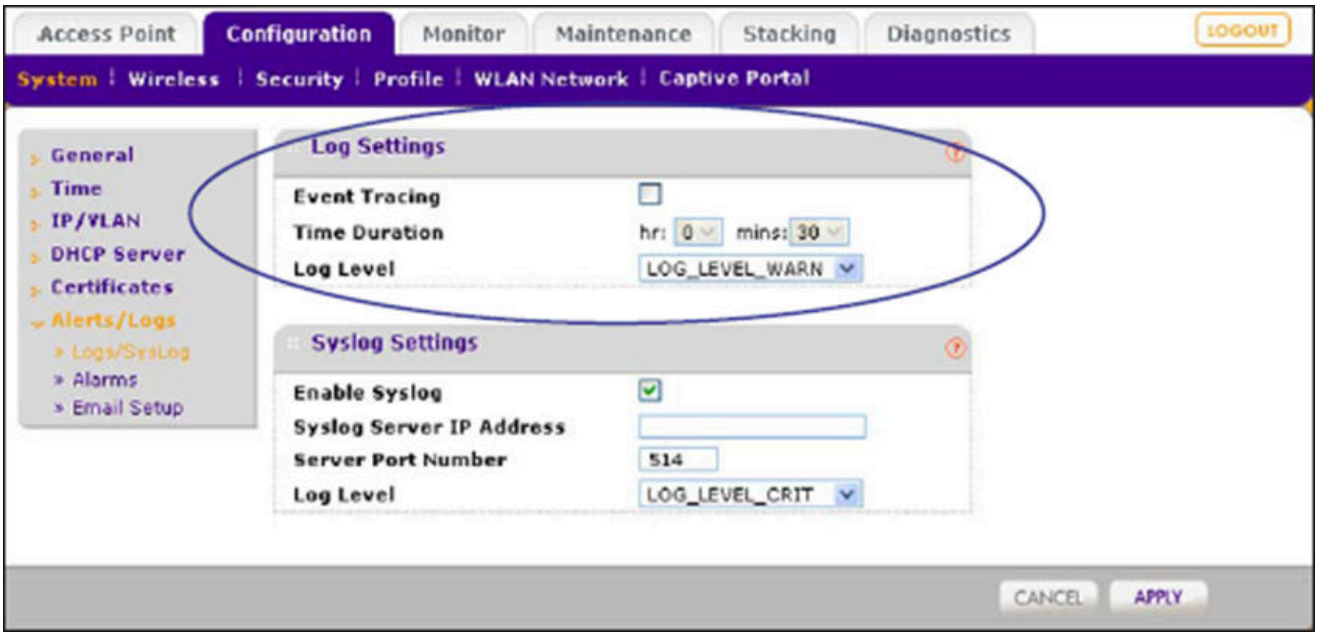
For the logs, you can either configure event tracing or select a log level. These selections are mutually exclusive.

Event tracing can help you to debug the wireless network. Event tracing generates logs from the wireless controller and from all controlled access points and saves these logs in a file on the wireless controller. The file can become large quickly.

To configure the log settings and view the logs

1. Open a **web browser**. In the browser's **address field**, type the **http://** followed by the IP address that you assigned to the wireless controller. By default, the IP address is **192.168.0.250** (if you have not yet assigned another IP address to the wireless controller, type http://192.168.0.250) and wireless controller's login screen displays
2. Enter your **username** and **password** (if you have not yet personalized your username and password, enter **admin** for both username and password, in lowercase letters)
3. Click **Login** (wireless controller's web management interface opens and displays the **Summary** screen)

4. Select **Configuration > System > Alerts/Logs > Logs/Syslog** (the *Log Settings* screen displays)



5. In the **Log Settings** section of the screen, configure either event tracing or a log level (these selections are mutually exclusive)

A) **Event tracing**. To configure event tracing, please follow the steps bellow:

i. Select the **Event Tracing** check box

ii. Next to **Time Duration**, use the menus to specify the period during which event tracing should occur

B) **Log level**. From the Log Level menu, select one of the following levels:

i. **LOG_LEVEL_CRIT** - Critical errors only are logged

ii. **LOG_LEVEL_ERR** - Noncritical errors and critical errors are logged

iii. **LOG_LEVEL_WARN** - Warnings, noncritical errors, and critical errors are logged

iv. **LOG_LEVEL_NOTICE** - Notifications, warnings, noncritical errors, and critical errors are logged

v. **LOG_LEVEL_INFO** - Informational messages, notifications, warnings, noncritical errors, and critical errors are logged

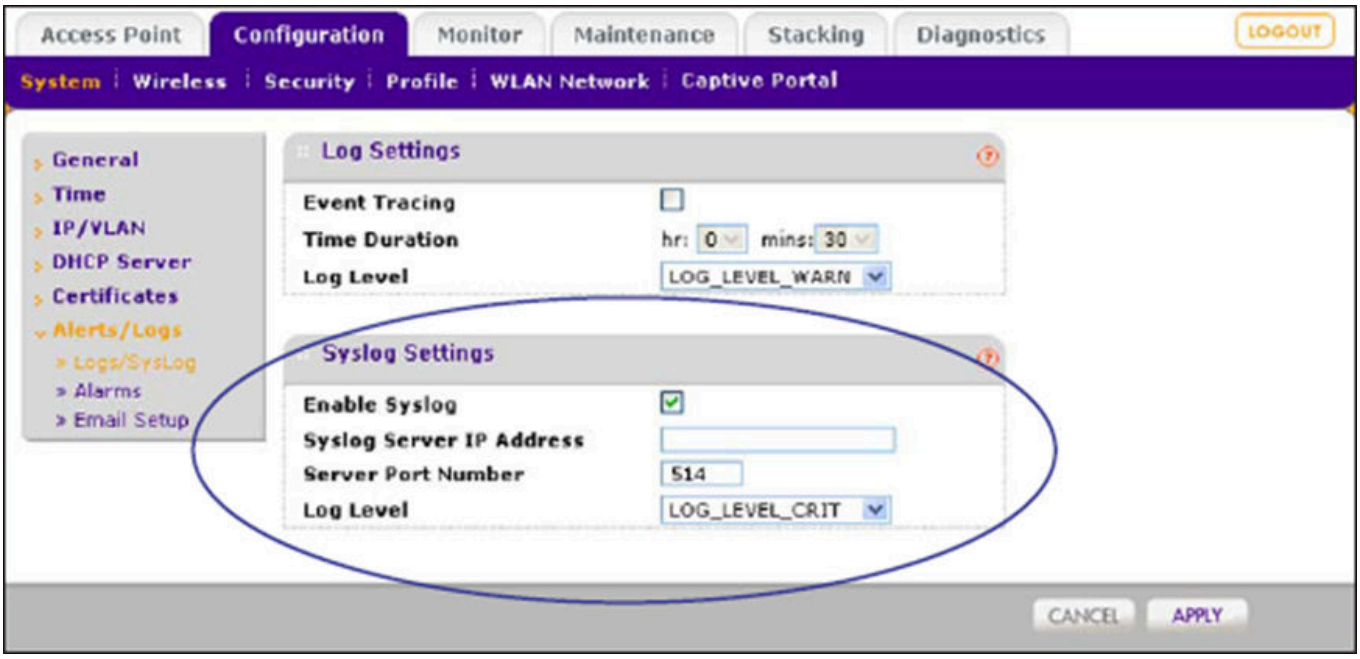
6. Click **Apply**

Configure Syslog Settings

This screen lets you configure the settings to connect to a syslog server if you have one configured in your network (before you configure the IP address of the syslog server on the wireless controller, make sure that you have set up a syslog server, such as a computer running a syslog service and that the syslog server is available on the network).

To configure syslog settings, please follow the steps bellow:

1. Open a **web browser**. In the browser's **address field**, type the **http://** followed by the IP address that you assigned to the wireless controller. By default, the IP address is **192.168.0.250** (if you have not yet assigned another IP address to the wireless controller, type http://192.168.0.250) and wireless controller's login screen displays.
2. Enter your **username** and **password** (If you have not yet personalized your username and password, enter **admin** for both username and password, in lowercase letters)
3. Click **Login** (wireless controller's web management interface opens and displays the **Summary** screen)
4. Select **Configuration > System > Alerts/Logs > Logs/Syslog** (the *Log Settings* screen displays)



5. In the **Syslog Settings** section of the screen, configure the settings as described in the below table:

Setting	Description
Enable Syslog	Enable the syslog settings if you have a syslog server on your network
Syslog Server IP Address	Enter the **CYBERQUEST IP address** to send all syslogs if the **Enable Syslog** check box is selected (before you configure the IP address of the CYBERQUEST server on the wireless controller, make sure that you have set up a syslog server, such as a computer running a syslog service and that the syslog server is available on the network)
Server Port Number	Enter port **5140 UDP** at which your syslog server is configured to listen to requests
Log Level	From the *Log Level* menu, select one of the following levels: •**LOG_LEVEL_CRIT**. Critical errors only are logged •**LOG_LEVEL_ERR**. Noncritical errors and critical errors are logged •**LOG_LEVEL_WARN**. Warnings, noncritical errors, and critical errors are logged •**LOG_LEVEL_NOTICE**. Notifications, warnings, noncritical errors, and critical errors are logged •**LOG_LEVEL_INFO**. Informational messages, notifications, warnings, noncritical errors, and critical errors are logged

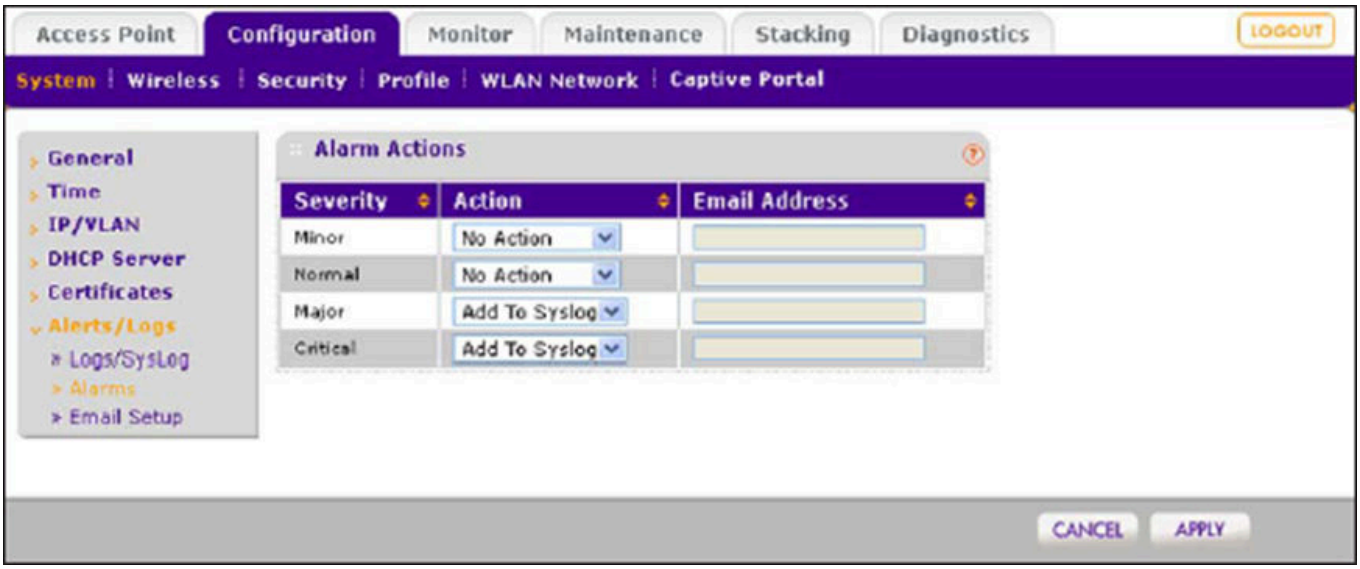
6. Click **Apply**

Configure Alarm Notification Settings

You can classify certain events as critical, major, normal, or minor. Some events you can classify only as critical or major. For example, on the RF Management screen, you can specify whether a coverage hole should be classified as critical or major.

To configure alarm actions, please follow the steps bellow:

1. Open a **web browser**. In the browser's **address field**, type the **http://** followed by the IP address that you assigned to the wireless controller. By default, the IP address is **192.168.0.250** (if you have not yet assigned another IP address to the wireless controller, type http://192.168.0.250) and wireless controller's login screen displays.
2. Enter your **username** and **password** (If you have not yet personalized your username and password, enter **admin** for both username and password, in lowercase letters)
3. Click **Login** (wireless controller's web management interface opens and displays the **Summary** screen)
4. Select **Configuration > System > Alerts/Logs > Alarms** (the *Alarms Actions* screen displays)



5. For each **alarm severity** (*Minor, Normal, Major, and Critical*), select the desired action from its corresponding **Action** menu:
   - **No Action**: when the alarm occurs, no action is taken
   - **Add to Syslog**: when the alarm occurs, wireless controller adds an entry to the syslog
   - **Send Email**: when the alarm occurs, wireless controller sends an email
6. For each alarm severity for which you have selected **Send Email** option in the previous step, enter an **email address**
7. Click **Apply**

How-to · How to configure NGNIX to send logs to CQ Server

Follow these steps to configure NGNIX to send logs to CYBERQUEST:

Add the following lines to the Nginx server configuration file ***(/etc/nginx/nginx.conf)*** in the "***Logging Settings***" section:

```
access_log syslog:server=IP Server CQ:5140,facility=local7,tag=nginx,severity=info;
```

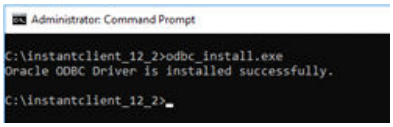
```
log_format main '$remote_addr $server_name $remote_user [$time_local] "$request" $status $body_bytes_sent "$http_refe
rer" "$http_user_agent" "$http_x_forwarded_for" $server_port $upstream_bytes_received "$sent_http_content_type" $host
"$https" "$http_cookie"';
```

How-to · How to configure ODBC client to collect from Oracle DB instances

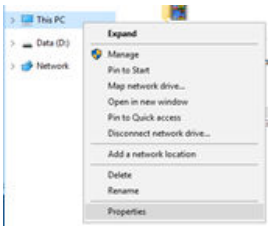
To collect log events from a Oracle database audit table, the following prerequisits must be met:

1. Download **instantclient-basic-nt-12.2.0.1.0.zip** (https://www.oracle.com/database/technologies/instant-client/winx64-64-downloads.html#license-lightbox) and **instantclient-odbc-nt-12.2.0.1.0.zip** (https://www.oracle.com/database/technologies/instant-client/winx64-64-downloads.html#license-lightbox)
2. Extract both archives to **C:\instantclient_12_2**
3. Open **CMD** Command Prompt as *Administrator*

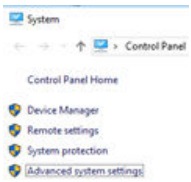
4. Run **odbc_install.exe**



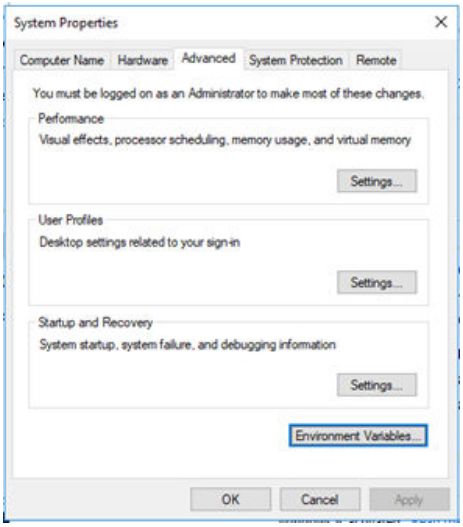
5. Open **Computer Proprieties**



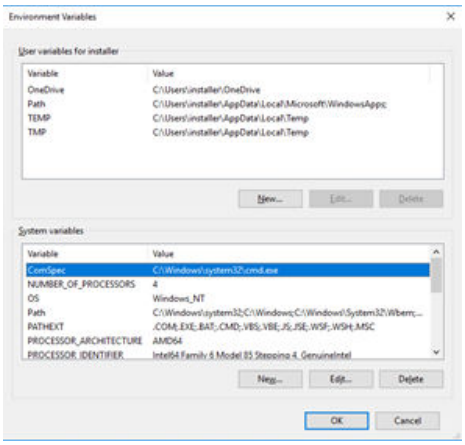
6. Go to **Advanced system settings**

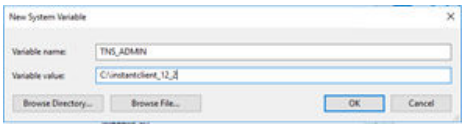


7. Open **Environment Variables**

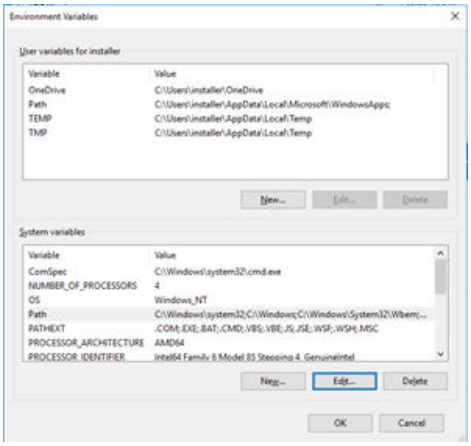


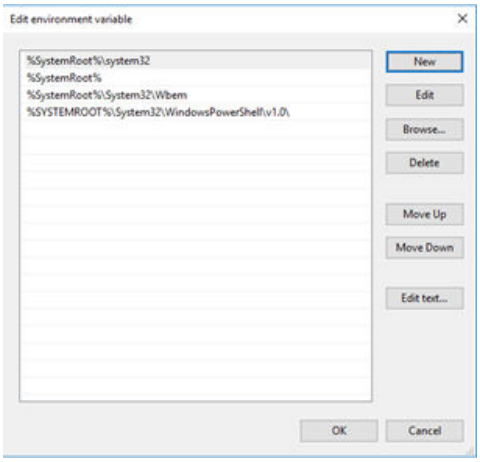
8. In **System Variables** edit/add *TNS_ADMIN* with value: *C:\instantclient_12_2*

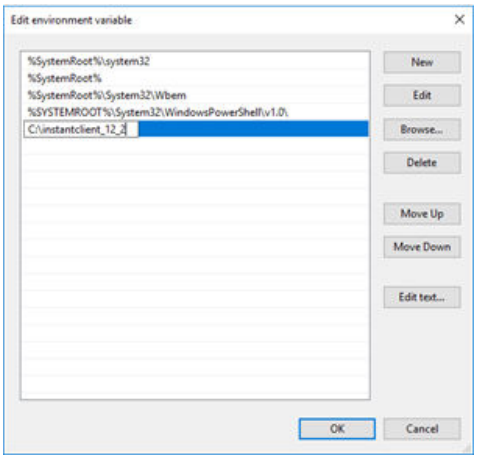




9. In **Path** tab add *C:\instantclient_12_2*







0. Install **Microsoft Visual C++ 2013 X86 Redistributable 12.0.40660 (https://www.microsoft.com/en-us/download/confirmation.aspx?id=40784)**

11. Create file *tnsnames.ora* in folder **C:\instantclient_12_2** and edit it with *TNS Instance setting*

dbInstance=

(description=

```
(address_list=
```

(address = (protocol = TCP) (host=)(port=))

)

(connect_data=

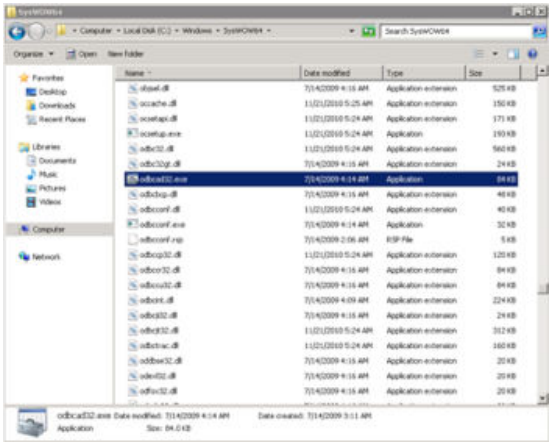
(service_name= dbInstance)

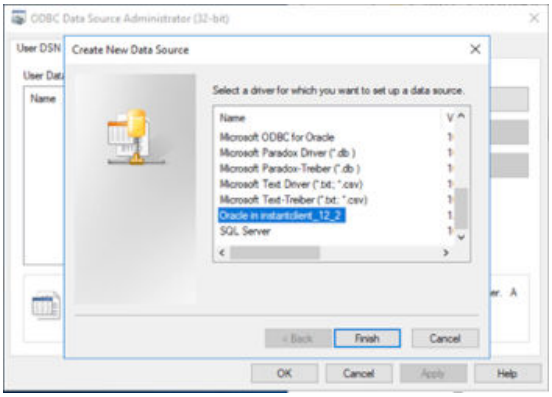
)

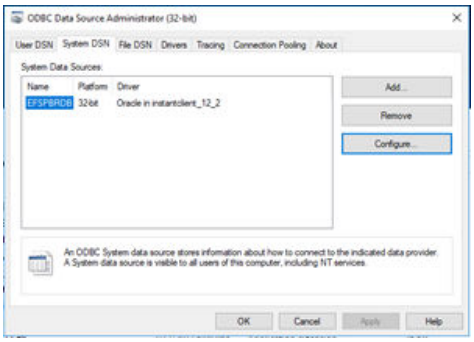
)

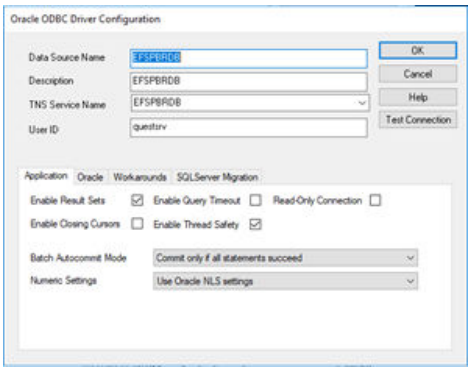
2. Navigate to *C:|Windows|SysWOW64* and run **odbcad32.exe**

3. **Setup** as shown below













How-to · How to configure Office365 to send logs to CQ Server

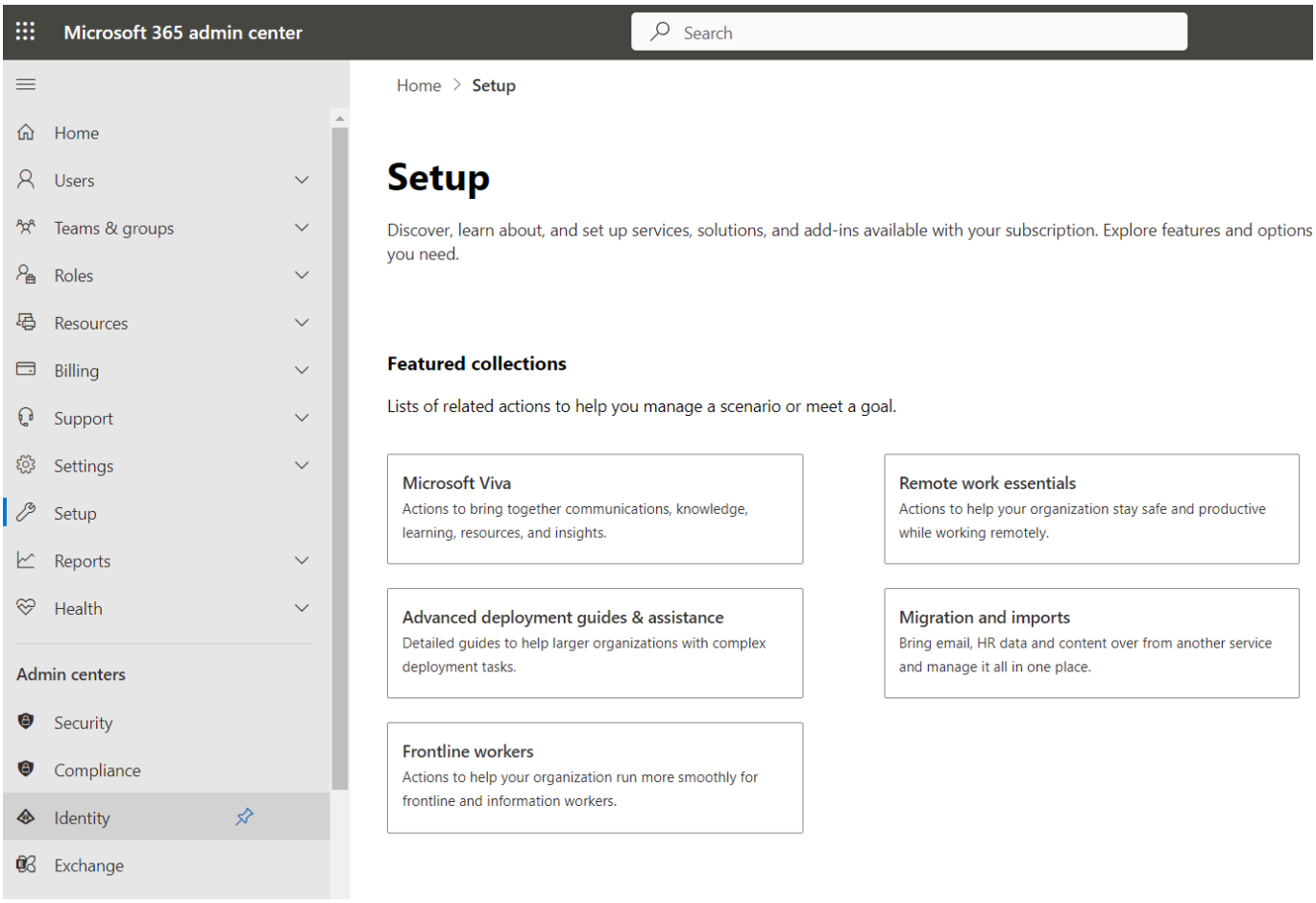
This guide describes the procedure for audit activation on Office365 application.

To collect logs from the Office 365 application, we need to follow the following steps:

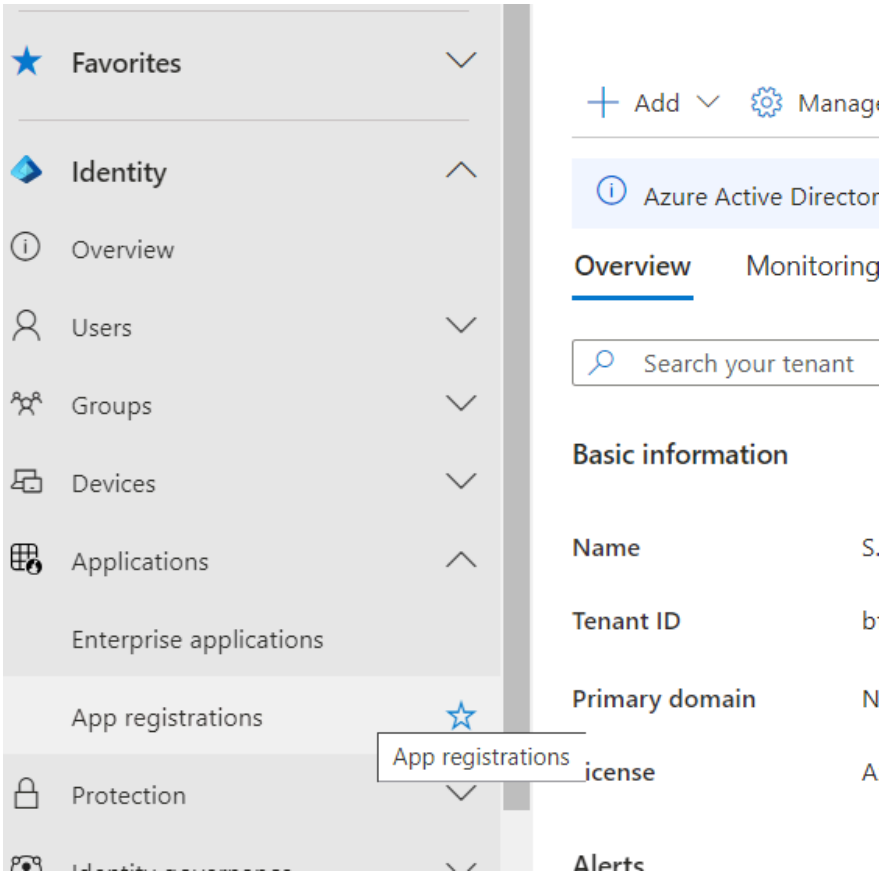
Step 1 - Registering the CQ Application in Office 365

A.Authentication in the **Office 365 admin center**

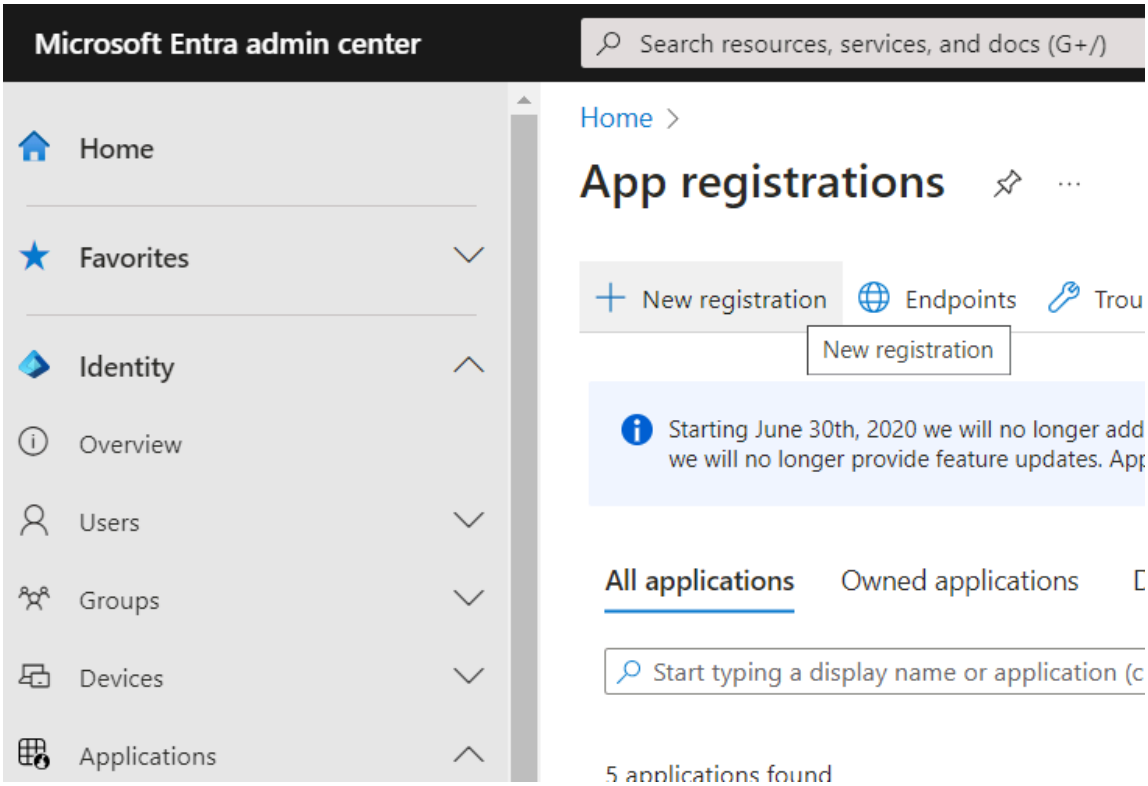
B.Select **Home** > **Setup** > **Identity** page



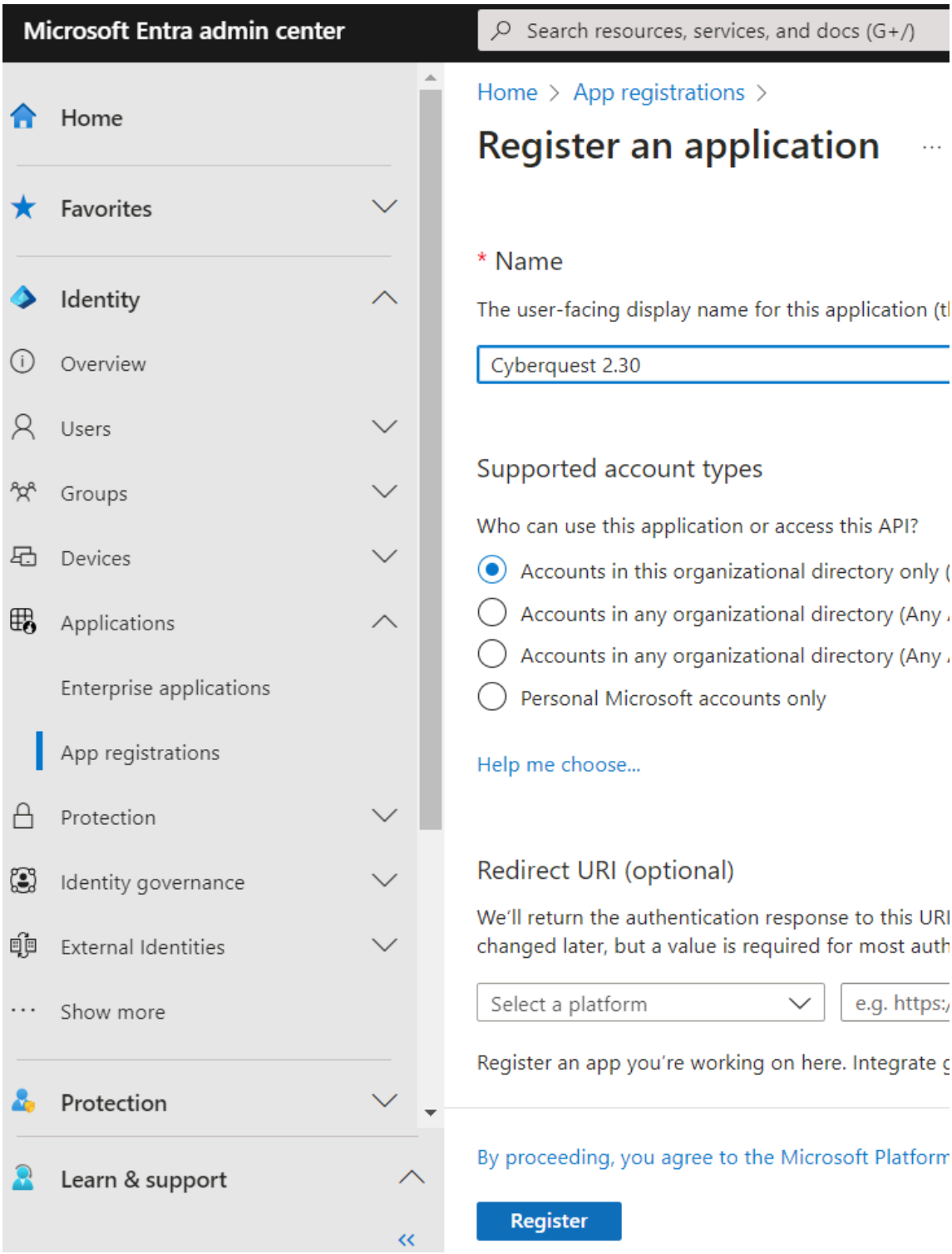
C.Select **Applications** > **App registrations**



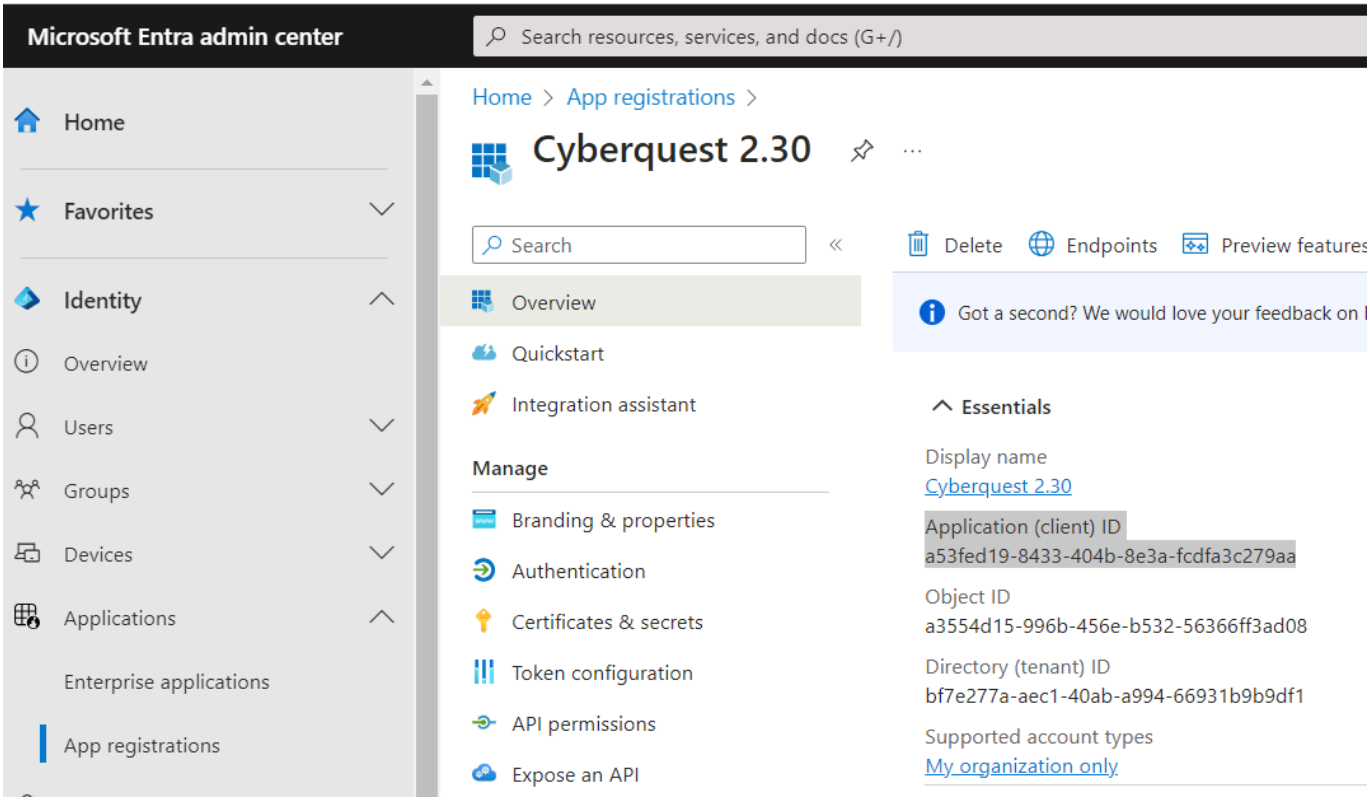
D.Click on the **New registration** button



E.Complete the application **Name**, select **Supported account types** and press the **Register** button



The page with what you registered earlier opens:



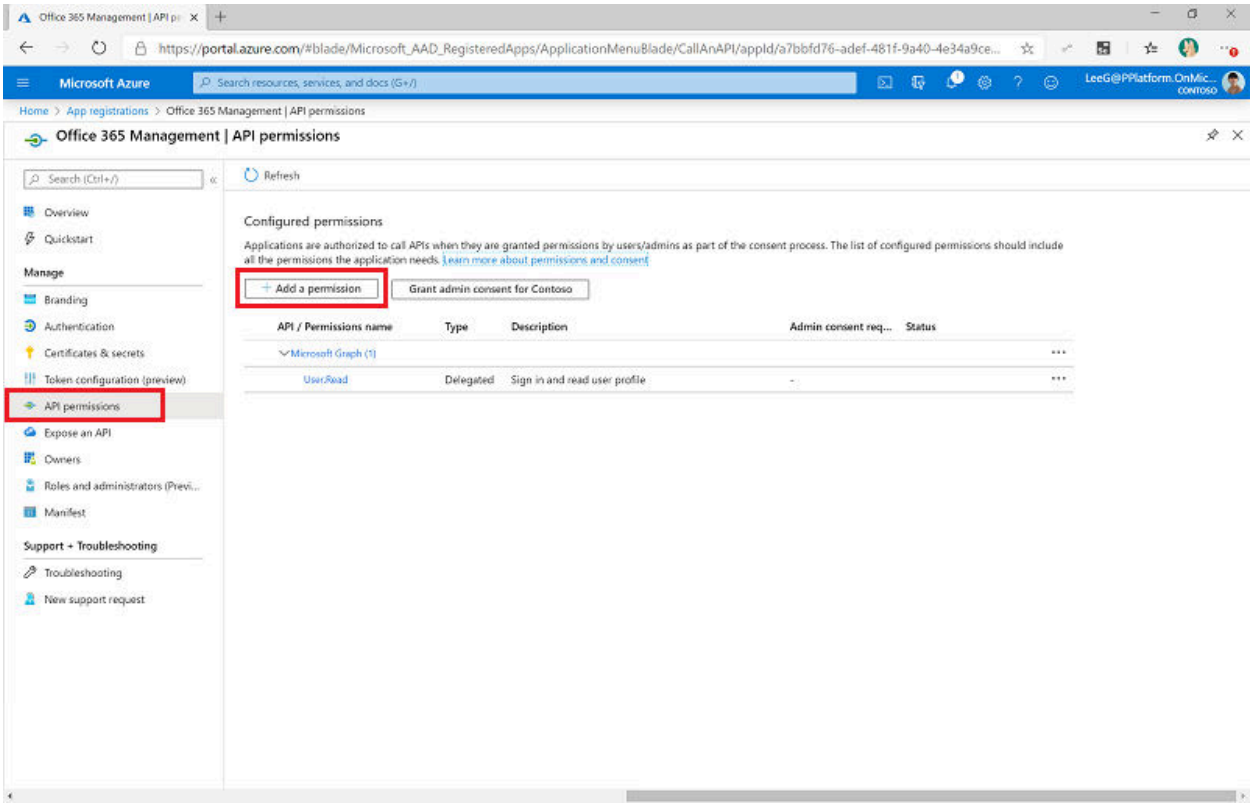
You need to copy the fields below:

a)**Application (client) ID**

b)**Directory (tenant) ID**

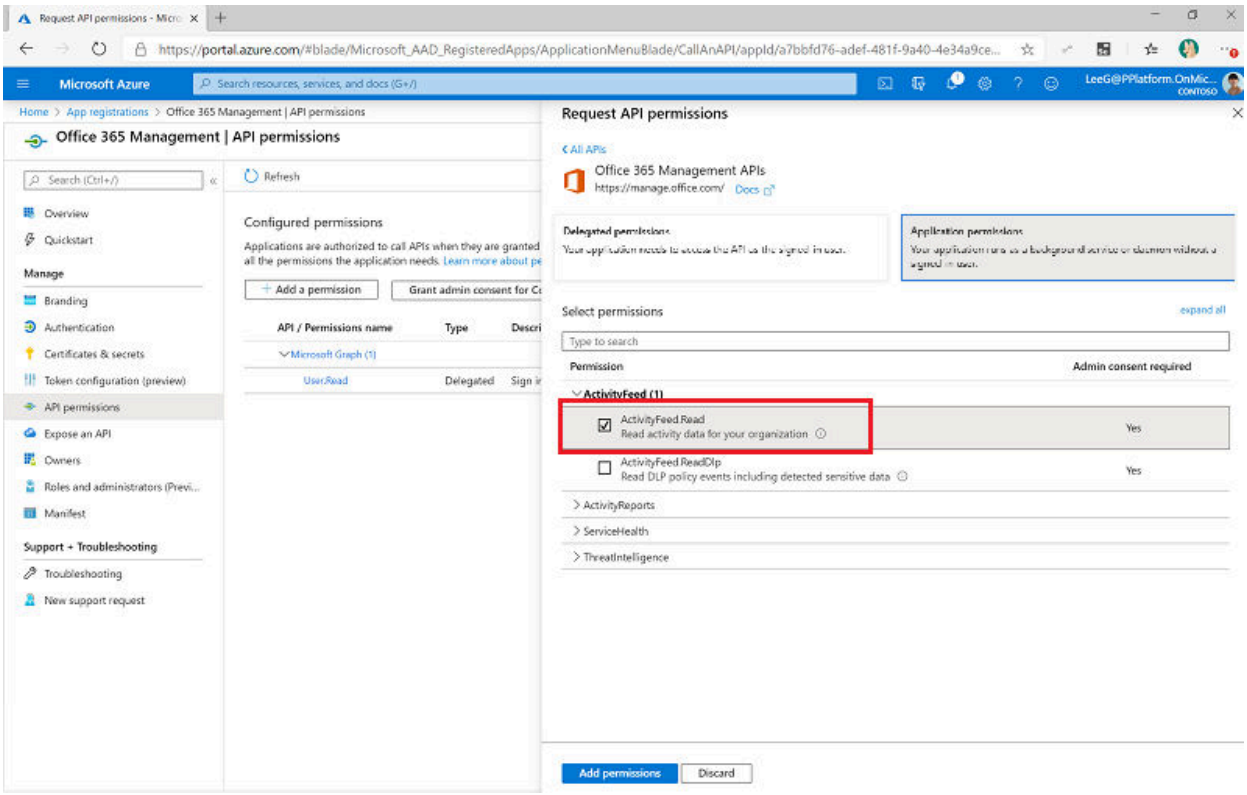
Step 2 - API Permissions

A.Select **API Permissions** > **+ Add a permission**



B.Select **Office 365 Management API** and configure permissions as follows:

1.Select **Application permissions**, and then select **ActivityFeed.Read**.



2.Select **Add permissions**.

C.Select **Grant Admin Consent for (your organization)**. Prerequisites: [Grant tenant-wide admin consent to an application (https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/grant-admin-consent#prerequisites)]

The API permissions now reflect delegated **ActivityFeed.Read** with a status of **Granted for (your organization)**.

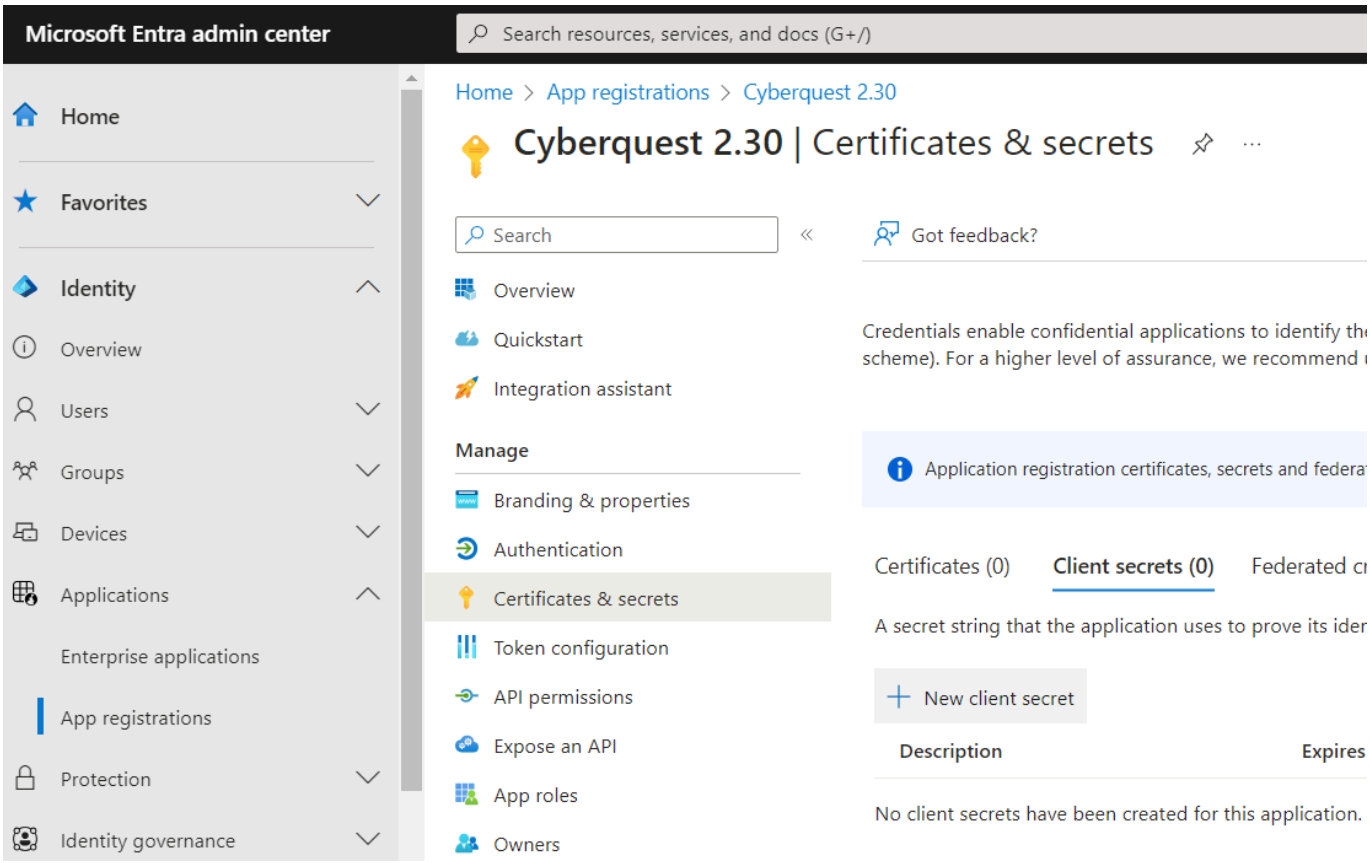
Reference:[link (https://learn.microsoft.com/en-us/power-platform/guidance/coe/setup-auditlog-http)]

Step 3 - Creating the Secret Key

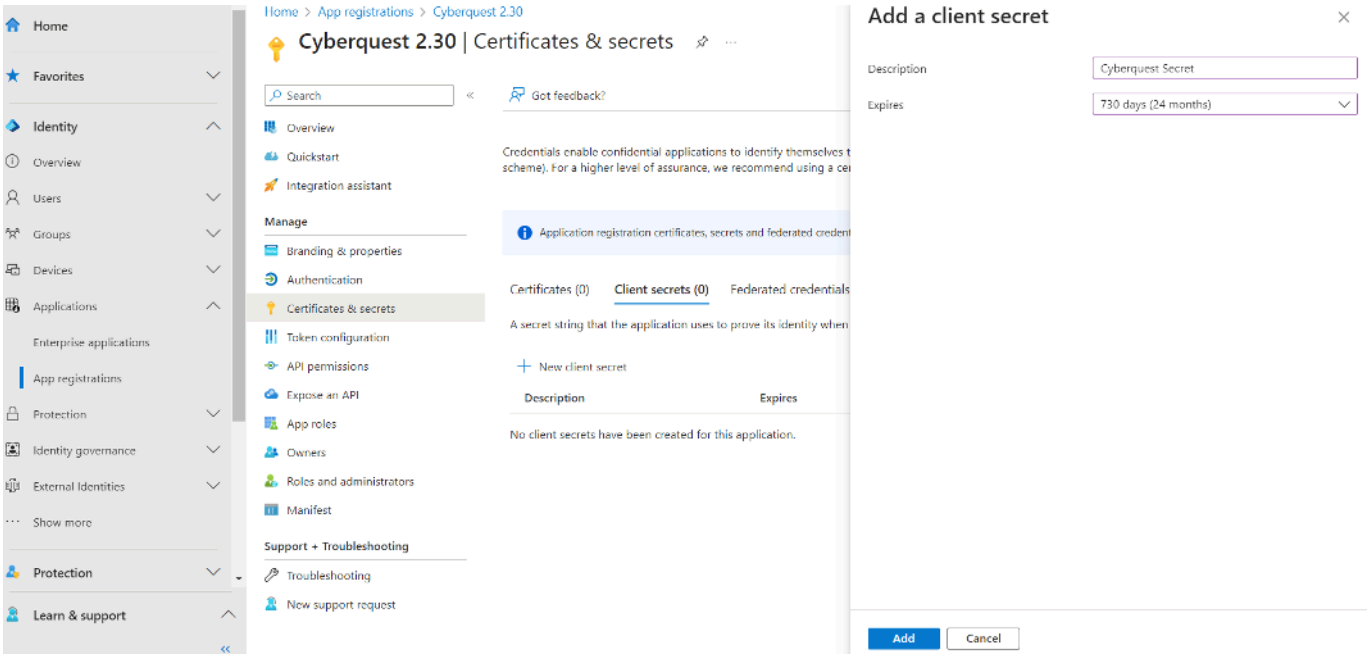
A.Select **Home** > **App Registrations** page and choose the application name created in Step 1

B.Select **Manage** > **Certificates & secrets** > **Client secrets** page

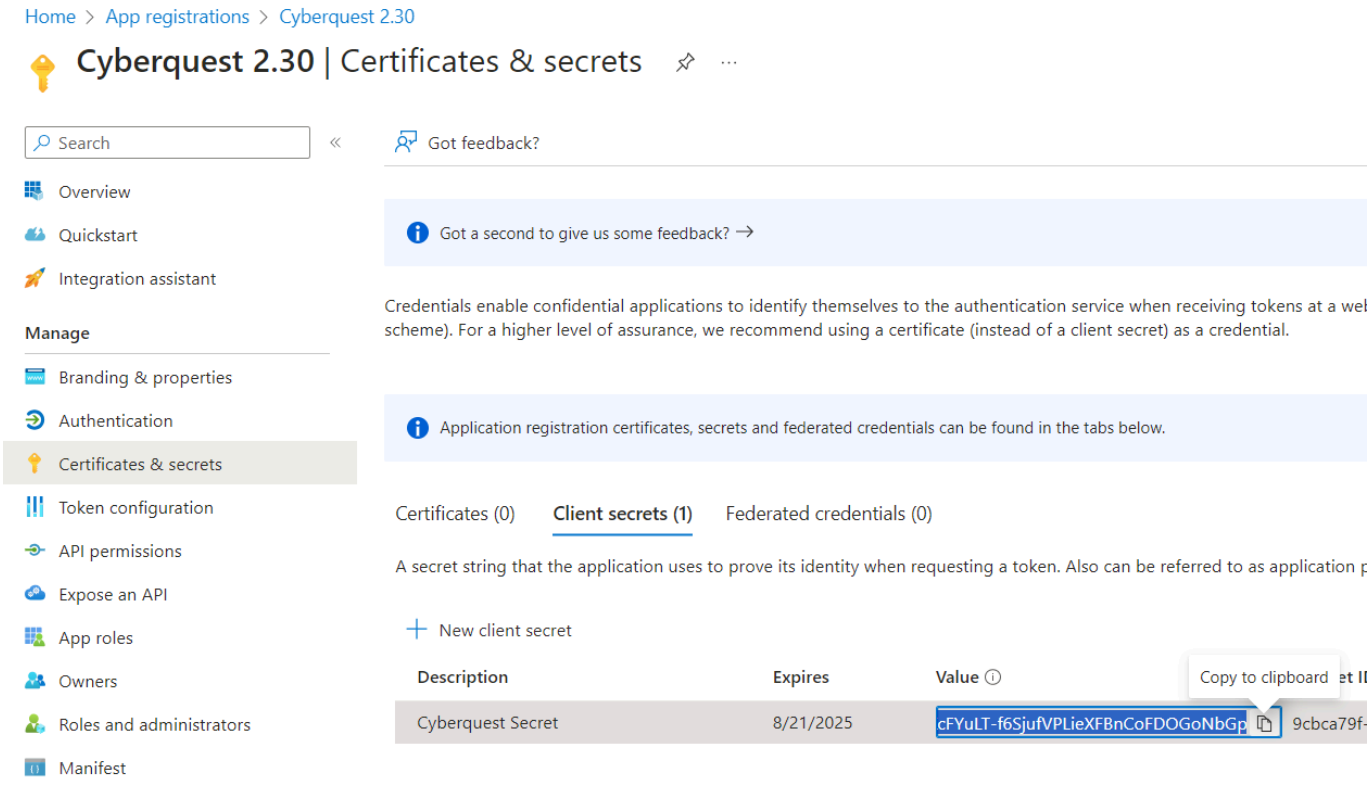
C.Click on the **New client secret** button



D.Complete the **Description**, select the **Expire** period and click on the **Add** button



Copy the **secret key** from the **Value** field:



How-to · How to configure VmWare VCSA 6.7 to send logs to CQ Server IP Address on port 5140 UDP

The vCenter Server log events can be sent to a remote syslog server to conduct an analysis of the logs, and can be configured to send log files to a vCenter Server rather than storing them to a local disk. The recommended maximum numbers of supported hosts to collect logs from is 30.

To configure VmWare VCSA 6.7 to send logs to CYBERQUEST, please follow the steps bellow:

1. **Log in** to the *vCenter Server Management Interface* as root
2. In **vCenter Server Management Interface**, select *Syslog*
3. In **Forwarding Configuration** tab, click **Configure** if you do not have any configured remote syslog hosts, or click **Edit** if you have configured hosts
4. In **Create Forwarding Configuration** pane enter the CYBERQUEST server IP address of the destination host (maximum number of destination hosts is 3)
5. From the **Protocol** drop-down menu, select the **UDP** *protocol*
6. In **Port** text box, enter port number **5140** to use for communication with destination host
7. Click **Save**
8. Verify that remote syslog server is receiving messages
9. In **Forwarding Configuration** tab, click *Send Test Message*
0. Verify on remote syslog server that the test message was received

How-to · How to configure WSO2 to send logs to CYBERQUEST server IP Address on port 5140 UDP

In this document we will detail how to send WSO2 logs (on Windows machine) to CQ Server IP Address on port 5140.

1.Log in to the WSO2 server as Administrator

2.Edit the following file **log4j2.properties**. We find this file following this path:
C:\Program Files\WSO2\Identity Server\5.11.0\repository\conf

3.Add the **syslog** entry to the end of the line to use the syslog appender

Example:

#list of all appenders

appenders = CARBON_CONSOLE, CARBON_LOGFILE, AUDIT _LOGFILE, ATOMIKOS_LOGFILE, CARBON_TRACE_LOGFILE, DELETE_EVENT _LOGFILE, TRANSACTION_LOGFILE, osgi, **syslog**

4.To use the Syslog Appender follow the steps:

a) Uncomment the below lines to use the Syslog Appender:

```
appender.syslog.type = Syslog
appender.syslog.name = Syslog
appender.syslog.host = localhost
appender.syslog.port = 514
appender.syslog.layout.type = PatternLayout
appender.syslog.layout.pattern = [%d] [%tenantId] %5p {%c} - %mm%ex%n
appender.syslog.filter.threshold.type = ThresholdFilter
appender.syslog.filter.threshold.level = DEBUG
```

b) Add the line: **appender.syslog.protocol = udp**

c) Change the date-time format, add ServerName and tag.

Example:

appender.syslog.layout.pattern = **%d{yyyy-MM-dd'T'HH:mm:ss.SSSXXX} ServerName wso2is** [%tenantId] %5p {%c} - %mm%ex%n %t

Final result, in the **log4j2.properties** file should contain the following lines:

appender.syslog.type = syslog

appender.syslog.name= syslog

appender.syslog.host = CQ SERVER IP

appender.syslog.port = 5140

appender.syslog.protocol = udp

appender.syslog.layout.type = PatternLayout

appender.syslog.layout.pattern = %d{yyyy-MM-dd'T'HH:mm:ss.SSSXXX} ServerName wso2is [%tenantId] %5p {%c} - %mm%ex%n %t

appender.syslog.filter.threshold.type = ThresholdFilter

appender.syslog.filter.threshold.level = DEBUG

5.Uncomment the last line to add syslog appender to the root logger

Example:

#root loggers

rootLogger.level = INFO

rootLogger.appenderRef.CARBON_CONSOLE.ref = CARBON_CONSOLE

rootLogger.appenderRef.CARBON_LOGFILE.ref = CARBON_LOGFILE

rootLogger.appenderRef.PaxOsgi.ref = PaxOsgi

rootLogger.appenderRef.syslog.ref = syslog

6.**Save** the configuration file

How-to · How to enable MariaDB auditing

The following logs can be received from MariaDB:

Type	Description	Supported versions
CONNECT	Connects, disconnects and failed connects—including the error code	
QUERY	Queries executed and their results in plain text, including failed queries due to syntax or permission errors	
TABLE	Tables affected by query execution	
QUERY_DDL	Similar to `QUERY`, but filters only DDL-type queries (`CREATE`, `ALTER`, `DROP`, `RENAME` and `TRUNCATE` statements—except `CREATE/DROP [PROCEDURE / FUNCTION / USER]` and `RENAME USER` (they're not DDL)	5.5.42, 10.0.17, 10.1.4
QUERY_DML	Similar to `QUERY`, but filters only DML-type queries (`DO`, `CALL`, `LOAD DATA/XML`, `DELETE`, `INSERT`, `SELECT`, `UPDATE`, `HANDLER` and `REPLACE` statements)	5.5.42, 10.0.17, 10.1.4
QUERY_DML_NO_SELECT	Similar to `QUERY_DML`, but doesn't log SELECT queries. (since version 1.4.4) (`DO`, `CALL`, `LOAD DATA/XML`, `DELETE`, `INSERT`, `UPDATE`, `HANDLER` and `REPLACE` statements)	5.5.42, 10.0.17, 10.1.4
QUERY_DCL	Similar to `QUERY`, but filters only DCL-type queries (`CREATE USER`, `DROP USER`, `RENAME USER`, `GRANT`, `REVOKE` and `SET PASSWORD` statements)	5.5.43, 10.0.18, 10.1.5

To start logging events through MariaDB, follow these steps:

1. Enable the plugin in mariadb conf file (default: ***/etc/mysql/mariadb.conf.d/50-server.cnf***) with the command:

```
sudo nano /etc/mysql/mariadb.conf.d/50-server.cnf
```

2. Add the following lines below ([mariadb])

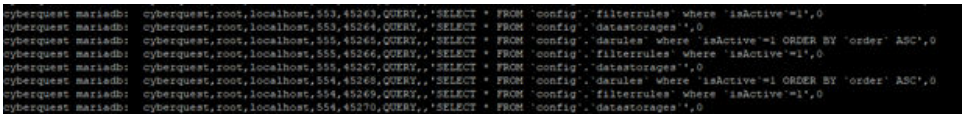
```
[mariadb]
plugin_load_add = server_audit
server_audit=FORCE_PLUS_PERMANENT
server_audit_logging=ON
server_audit_output_type=SYSLOG
server_audit_events=CONNECT,QUERY,TABLE,QUERY_DDL,QUERY_DML,QUERY_DCL
server-audit-syslog-facility=LOG_USER
server_audit_syslog_priority=LOG_INFO
server_audit_syslog_ident=mariadb
```

3. Restart the service in order to apply the changes with the command:

```
sudo systemctl restart mariadb.service
```

4. Check logs by tailing the syslog file (default: ***/var/log/syslog***) with the command:

```
sudo tail -f /var/log/syslog
```



How-to · How to enable or disable MS SQL Audit for MSSQL instance

Enable Audit on a MSSQL Instance

To enable Audit on a MSSQL Instance, follow the steps bellow:

1.Login to the instance where to **Enable Audit**



2.Open and execute the below scripts in this exact order:

a.**Create AND Enable Audit-CQ.sql**

```
USE [master]
GO
CREATE SERVER AUDIT [Audit-CQ]
TO APPLICATION_LOG
WITH
( QUEUE_DELAY = 1000
,ON_FAILURE = CONTINUE
,AUDIT_GUID = 'f12b8f4e-f428-43e4-9fe4-da481f07eca1'
)
ALTER SERVER AUDIT [Audit-CQ] WITH (STATE = ON)
GO
```

b.**Create AND Enable ServerAuditSpecification-Changes-CQ.sql**

```
USE [master]
GO
CREATE SERVER AUDIT SPECIFICATION [ServerAuditSpecification-Changes-CQ]
FOR SERVER AUDIT [Audit-CQ]
ADD (AUDIT_CHANGE_GROUP),
ADD (DATABASE_CHANGE_GROUP),
ADD (DATABASE_OBJECT_CHANGE_GROUP),
ADD (SCHEMA_OBJECT_CHANGE_GROUP)
WITH (STATE = ON)
GO
```

c.**Create AND Enable Audit-Permissions-Changes-CQ.sql**

```
USE [master]
GO
CREATE SERVER AUDIT [Audit-Permissions-Changes-CQ]
TO APPLICATION_LOG
WITH
( QUEUE_DELAY = 1000
,ON_FAILURE = CONTINUE
,AUDIT_GUID = '275cc430-362d-44eb-8e84-5f82e34b90b9'
)
ALTER SERVER AUDIT [Audit-Permissions-Changes-CQ] WITH (STATE = ON)
GO
```

d.**Create AND Enable Audit-ServerAuditSpecification-Permissions-Changes-CQ.sql**

```
USE [master]
GO
CREATE SERVER AUDIT SPECIFICATION [Permissions-Changes-CQ]
FOR SERVER AUDIT [Audit-Permissions-Changes-CQ]
ADD (DATABASE_PERMISSION_CHANGE_GROUP),
ADD (SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP),
ADD (DATABASE_OBJECT_OWNERSHIP_CHANGE_GROUP),
ADD (SERVER_OBJECT_OWNERSHIP_CHANGE_GROUP)
WITH (STATE = ON)
GO
```

3.**To configure login auditing, follow the steps bellow:**

a.In SQL Server Management Studio, connect to an instance of the SQL Server Database Engine with Object Explorer.

b.In Object Explorer, right-click the server name, and then click **Properties**.

c.On the **Security** page, under **Login** auditing, click the desired option and close the **Server Properties** page.

d.In Object Explorer, right-click the server name, and then click **Restart**.

Disable Audit on a MSSQL Instance

To **disable** Audit on a MSSQL Instance, follow the steps:

1.Login to the instance where to **Disable Audit**



2.Open and execute the below scripts in this exact order:

a.**Drop AND Disable Audit-CQ.sql**

```
USE [master]
GO
ALTER SERVER AUDIT [Audit-CQ] WITH (STATE = OFF)
GO
DROP SERVER AUDIT [Audit-CQ]
GO
```

b.**Drop AND Disable ServerAuditSpecification-Changes-CQ.sql**

```
USE [master]
GO
ALTER SERVER AUDIT SPECIFICATION ServerAuditSpecification-Changes-CQ]
WITH (STATE = OFF)
GO
DROP SERVER AUDIT SPECIFICATION ServerAuditSpecification-Changes-CQ]
GO
```

c.**Drop AND Disable Audit-Permissions-Changes-CQ.sql**

```
USE [master]
GO
ALTER SERVER AUDIT [Audit-Permissions-Changes-CQ] WITH (STATE = OFF)
GO
DROP SERVER AUDIT [Audit-Permissions-Changes-CQ]
GO
```

d.**Drop AND Disable Audit-ServerAuditSpecification-Permissions-Changes-CQ.sql**

```
USE [master]
GO
ALTER SERVER AUDIT SPECIFICATION [Permissions-Changes-CQ]
WITH (STATE = OFF)
GO
DROP SERVER AUDIT SPECIFICATION [Permissions-Changes-CQ]
GO
```

How-to · How to enable PostgreSQL auditing

The PostgreSQL server includes various system variables that specify the configuration of logging. All these variables are stored in the configuration file **postgresql.conf**. This file is by default stored in the directory: **/etc/postgresql/12/main/**.

Enabling Log Collector

You can enable log collector daemon by editing the **postgresql.conf**:

```
sudo nano /etc/postgresql/12/main/postgresql.conf
```

A.To configure log collector, perform the following actions:

1.Uncomment the variable **log_destination** and set to **syslog**.

```
# - Where to Log -
log_destination = 'syslog'
                                        # Valid values are combinations of
                                        # stderr, csvlog, syslog, and eventlog,
                                        # depending on platform.  csvlog
                                        # requires logging_collector to be on.
```

2.Uncomment the following lines:

```
syslog_facility = 'LOCAL7'
syslog_ident = 'postgres'
syslog_sequence_numbers = on
syslog_split_messages = on
```

3.Uncomment the following variables: **log_min_messages**, **log_min_messages** and **log_min_messages**. Set **log_min_messages** to **info**, **log_min_messages** to **error** and **log_min_messages** to **0**.

```
log_min_messages = info
                                        # values in order of decreasing detail:
                                        #   debug5
                                        #   debug4
                                        #   debug3
                                        #   debug2
                                        #   debug1
                                        #   info
                                        #   notice
                                        #   warning
                                        #   error
                                        #   log
                                        #   fatal
                                        #   panic

log_min_error_statement = error
                                        # values in order of decreasing detail:
                                        #   debug5
                                        #   debug4
                                        #   debug3
                                        #   debug2
                                        #   debug1
                                        #   info
                                        #   notice
                                        #   warning
                                        #   error
                                        #   log
                                        #   fatal
                                        #   panic (effectively off)
log_min_duration_statement = 0
                                        # -1 is disabled, 0 logs all statements
                                        # and their durations, > 0 logs only
                                        # statements running at least this number
                                        # of milliseconds
```

4.Uncomment the following lines and set to **on**:

```
log_connections = on
log_disconnections = on
```

5.Uncomment **log_statement** variable and set to **all**:

```
log_statement = 'all'
```

B.Configuring Log Collector Structure

You can configure the structure of each log record by various configuration variables. Firstly, let's set up a record header. The record prefix structure is determined by the variable **log_line_prefix**, which holds the ***printf*** style string. The following list shows the most important escape characters:

- **%t**: Timestamp without milliseconds (**%m** is with miliseconds). If you want to configure timestamp format to a specific local time then you can set up variable **log_timezone** to chosen geographical location. For example America/New_York, Europe/Paris, or any other name from the IANA timezone database .
- **%p**: Process ID.
- **%q**: If it is non-session process then stop record at this point.
- **%d**: Name of database.
- **%u**: User name.
- **%h**: Remote hostname or IP address. By default, the IP address is recorded. You can set up DNS translation to hostname by enabling variable **log_hostname** to value on. However, this setting is usually too expensive as it consumes a lot of

resources.

- **%a**: Application name.
- **%l**: Numbering the records in each session (every session start from number 1).

Set **log_line_prefix** variable to: **%m [%p] %q%u@%d %r**

```
log_line_prefix = '%m [%p] %q%u@%d %r '
                                        # special values:
                                        #   %a = application name
                                        #   %u = user name
                                        #   %d = database name
                                        #   %r = remote host and port
                                        #   %h = remote host
                                        #   %p = process ID
                                        #   %t = timestamp without milliseconds
                                        #   %m = timestamp with milliseconds
                                        #   %n = timestamp with milliseconds (as a Unix epoch)
                                        #   %i = command tag
                                        #   %e = SQL state
                                        #   %c = session ID
                                        #   %l = session line number
                                        #   %s = session start timestamp
                                        #   %v = virtual transaction ID
                                        #   %x = transaction ID (0 if none)
                                        #   %q = stop here in non-session
                                        #        processes
```

C.To apply the new configuration rules then you must restart the PostgreSQL server:

```
sudo systemctl restart postgresql.service
```

Summary:

If you set up all described variables in **postgresql.conf** and restart the server then you can view the content of the new logs.

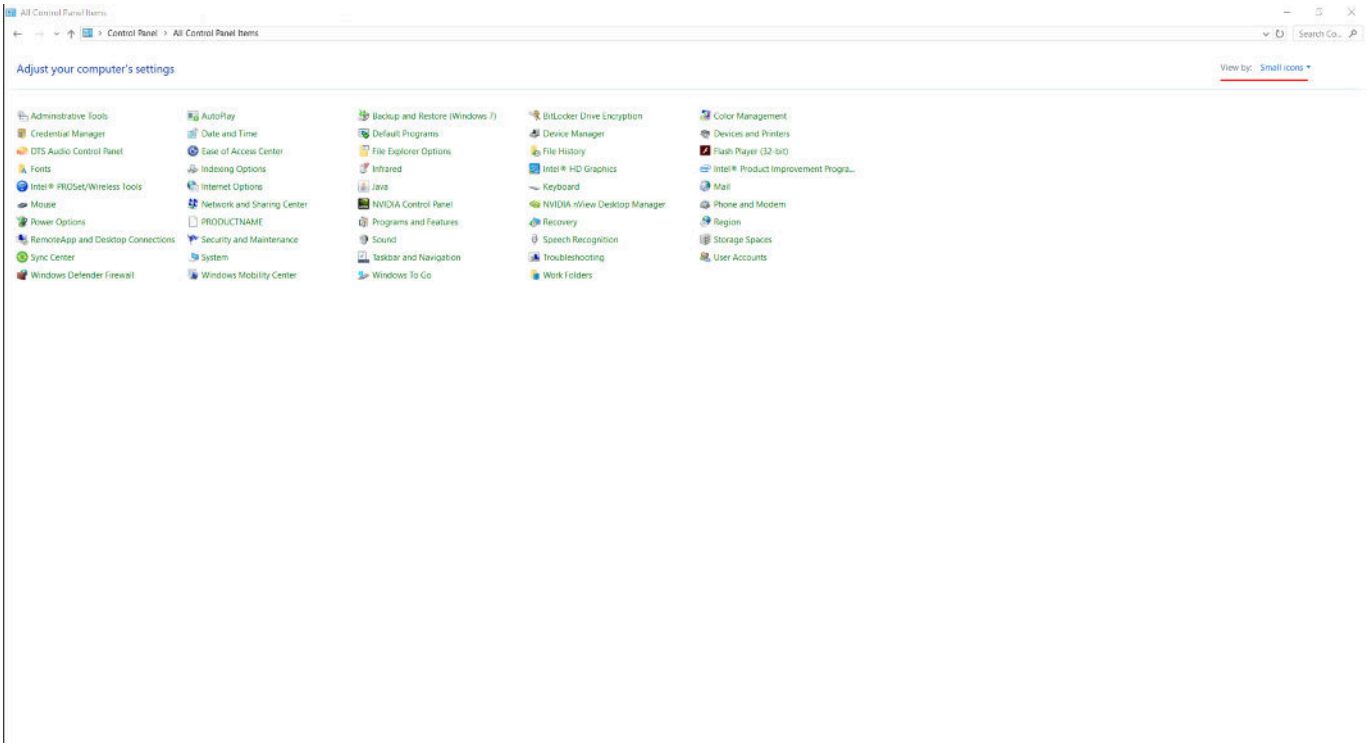
For example, we will use following **postgresql.conf** configuration:

```
log_destination = 'syslog'
syslog_facility = 'LOCAL7'
syslog_ident = 'postgres'
syslog_sequence_numbers = on
syslog_split_messages = on
log_min_messages = info
log_min_error_statement = error
log_min_duration_statement = 0
log_connections = on
log_disconnections = on
log_statement = 'all'
log_line_prefix = '%m [%p] %q%u@%d %r '
```

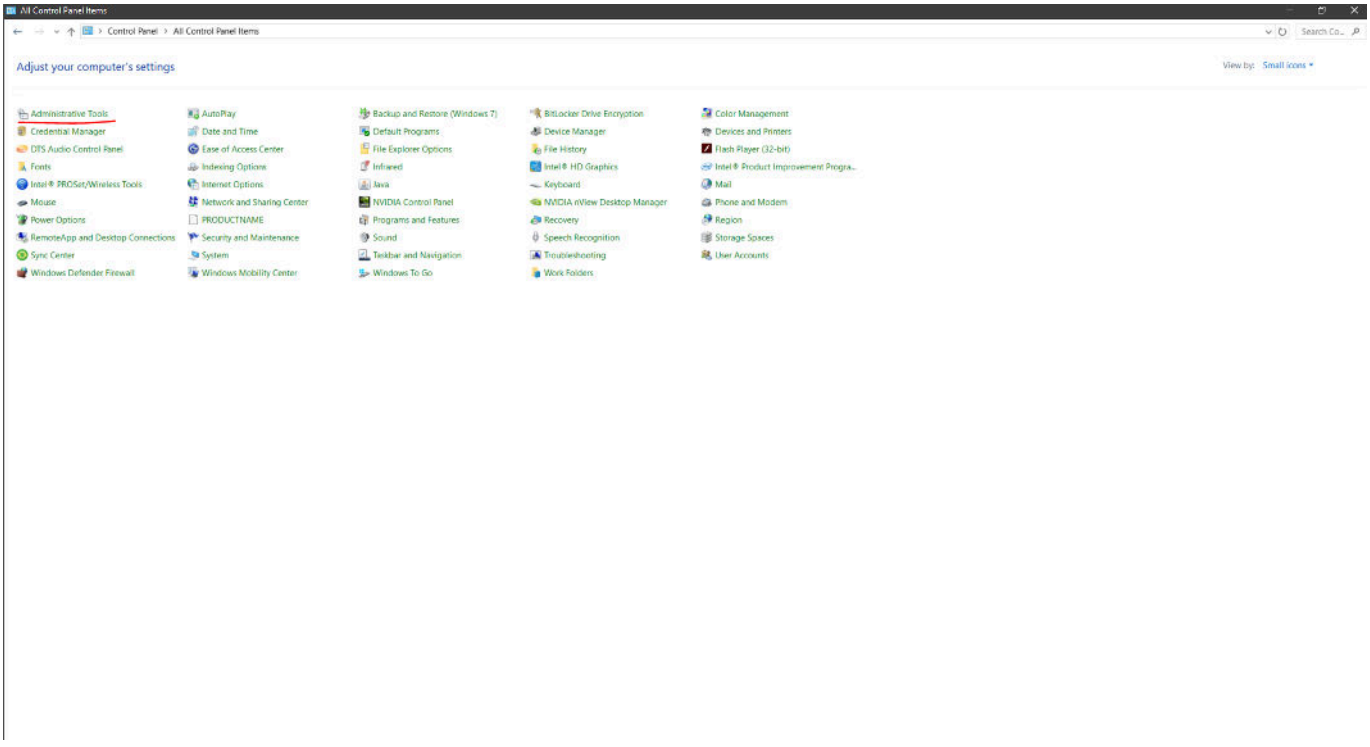
How-to · How to enable Print Service audit

Follow the instructions as shown in the images below to enable print service audit.

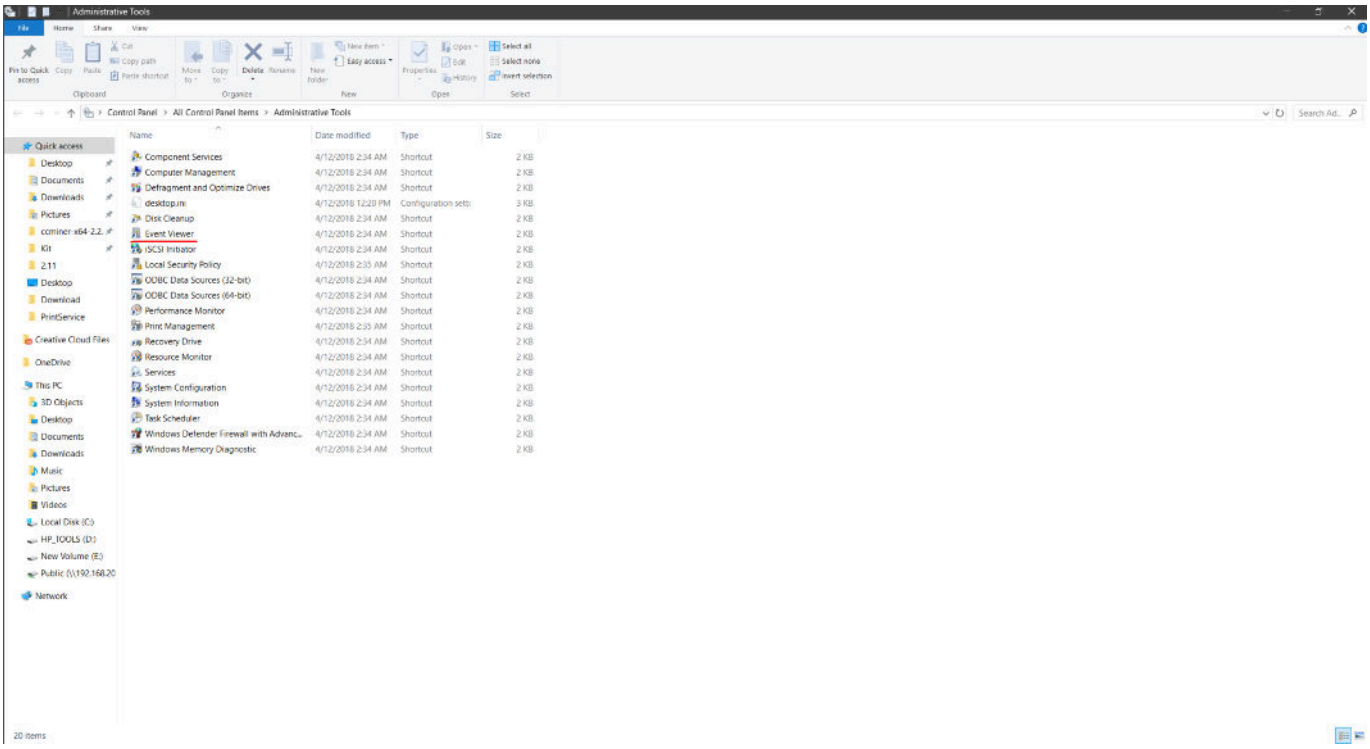
A.Open **Control Panel** and choose **Small icons** view



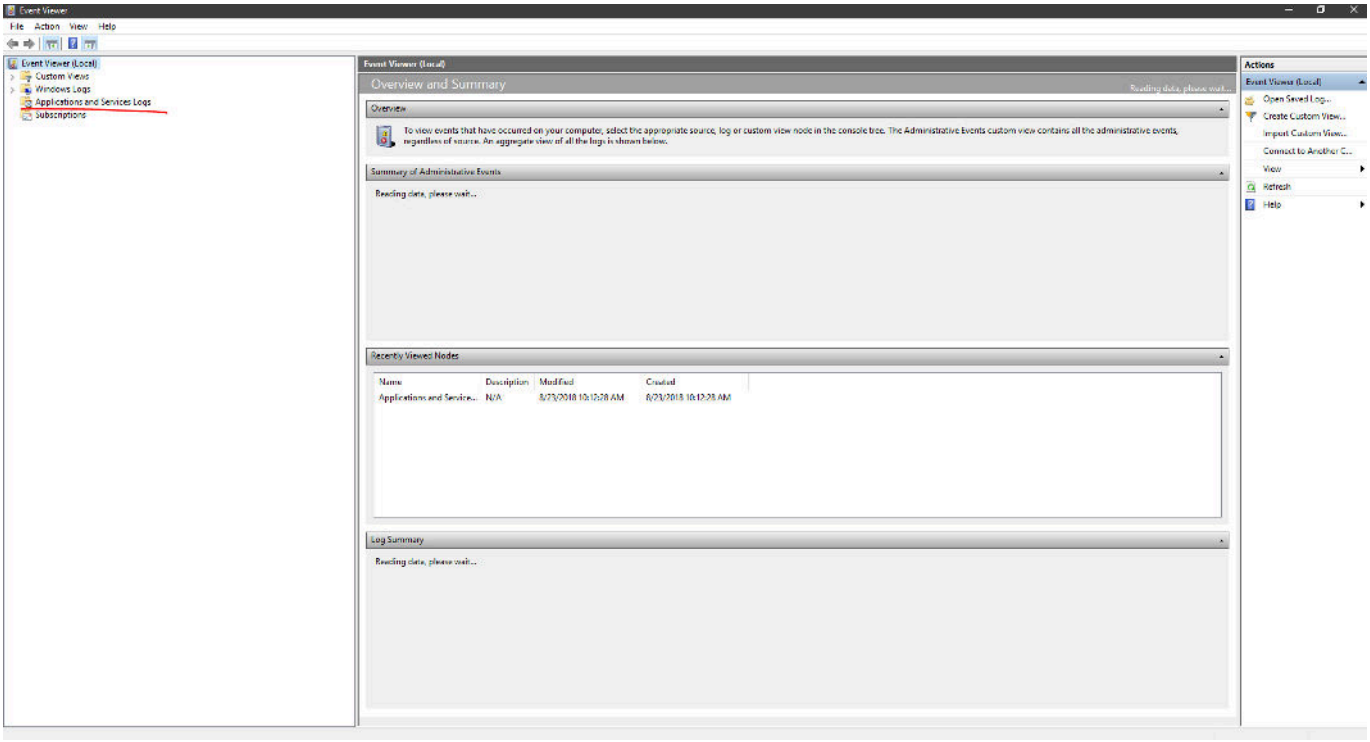
B.Open **Administrative Tools**



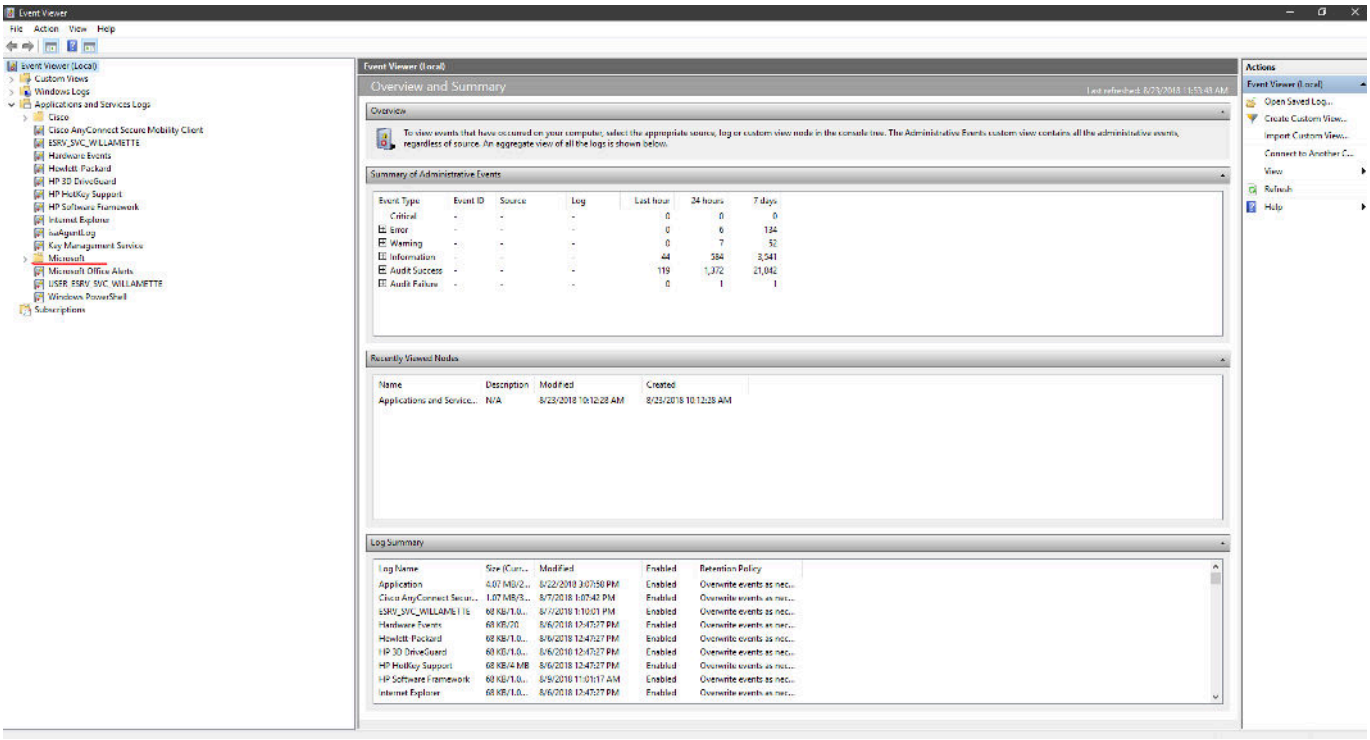
C.Choose **Event Viewer**



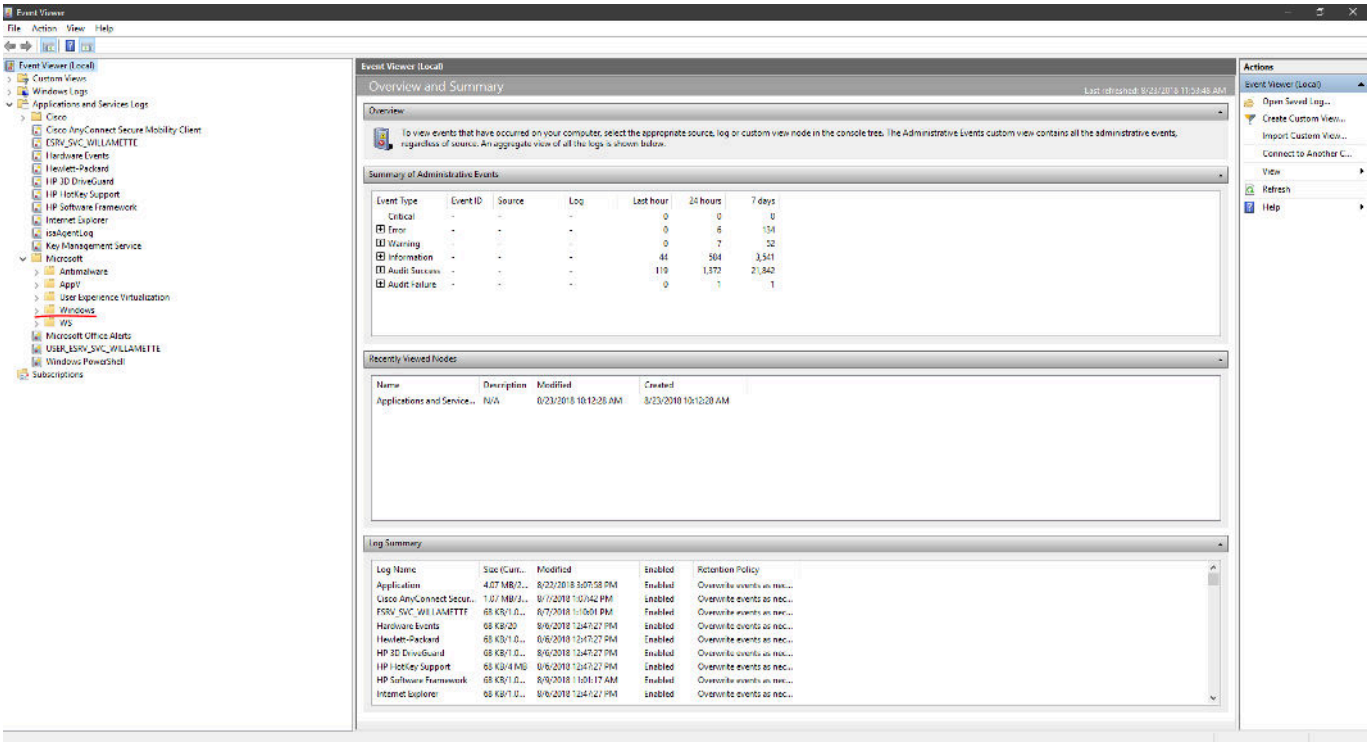
D.Click on **Applications and Services Logs**



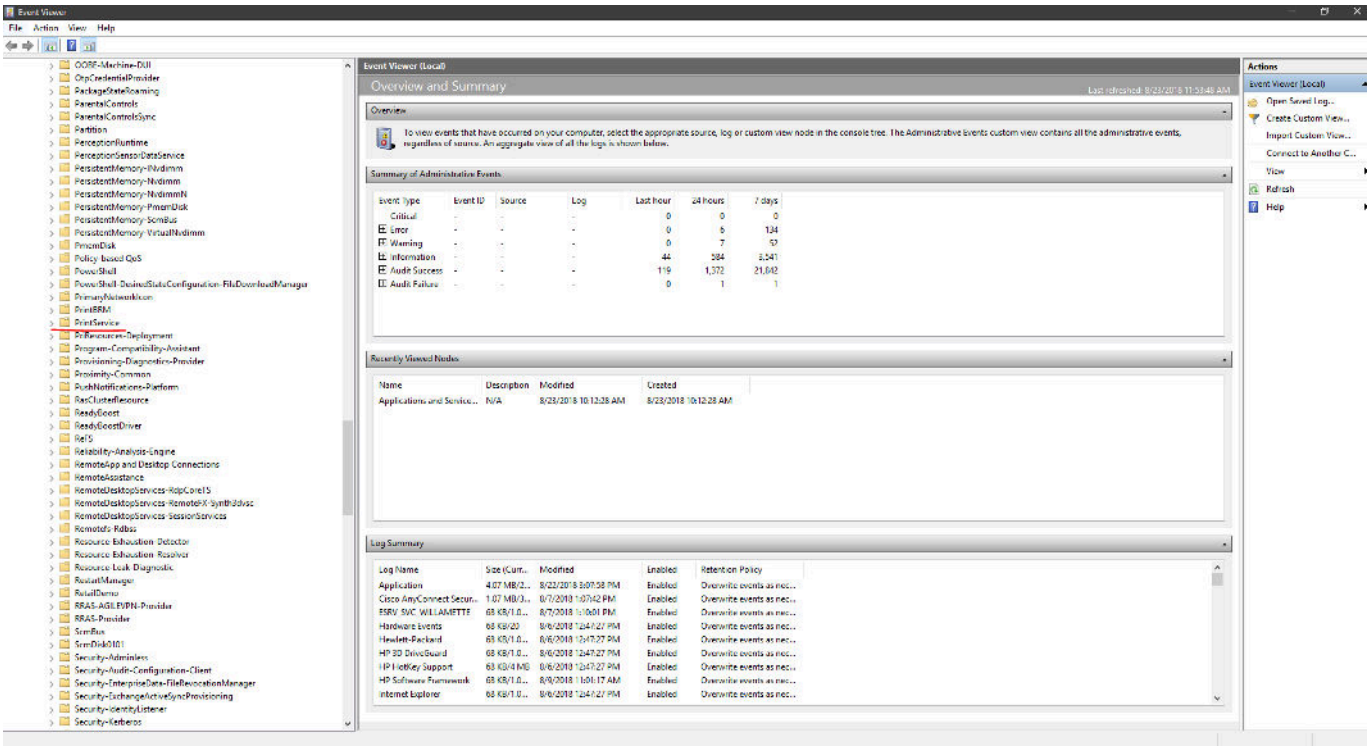
E.Expand **Microsoft** folder



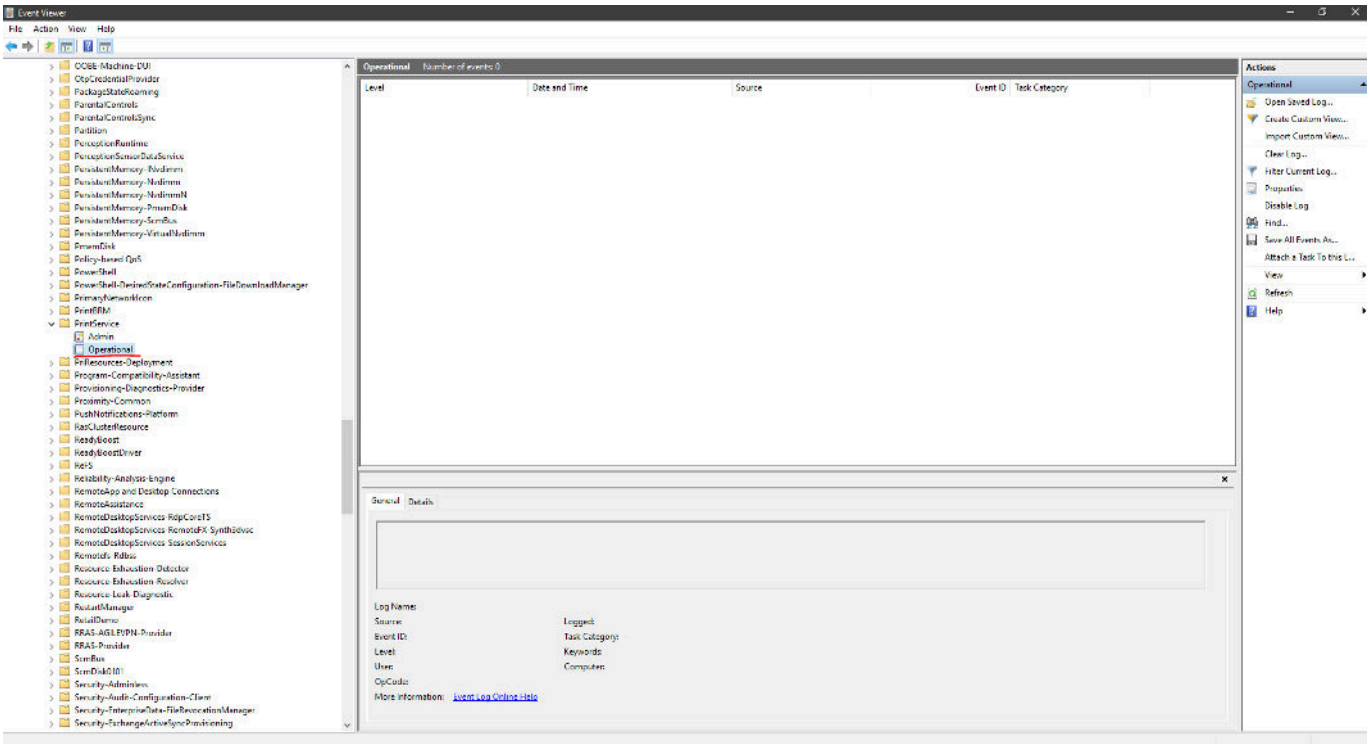
F.Choose **Windows** folder



G.Click on **PrintService**



H.Choose **Operational**



How-to · How to enable the Audit service for Linux

To enable the Audit service for Linux OS, please follow the steps bellow:

1.1 To **enable auditd** on ***Debian/Ubuntu*** based systems, run the following command:

```
sudo apt install -y auditd audispd-plugins
```

1.2 To install on ***RedHat/Centos*** based systems, run the following command:

```
yum install audispd-plugins
```

2.Configure a minimum predefined rule set

```
echo '-w /etc/passwd -p wa -k password_changes\
-w /etc/groups -p wa -k groups_changes\
-w /etc/ -pa -k configuration_changes' > /etc/audit/rules.d/cq.rules
```

3.**Forward all logs** via auditsp to syslog

```
nano /etc/audisp/plugins.d/syslog.conf
set
active = yes
```

4.**Restart** audit service using the following command:

```
systemctl restart auditd.service
```

5.Verify that local machine syslog forwards to CQ Data Server

Once configured, start the service to collect Audit information and store it in the log files, using the following command as the **root** user to **start auditd**:

```
service auditd start
```

Other actions can be performed on auditd using the *service auditd action* command, where *action* can be one of the following:

- **stop**: stops auditd
- **restart**: restarts auditd
- **reload** or **force-reload**: reloads auditd configuration from the */etc/audit/auditd.conf* file
- **rotate**: rotates log files in */var/log/audit/* directory
- **resume**: resumes logging of audit events after it has been previously suspended
- **condrestart** or **try-restart**: restarts auditd only if it is already running
- **status**: displays the running status of auditd

How-to · How to integrate HR system in CYBERQUEST

To collect log events from HR system, the following steps must be met:

- Export the logs from HR system into CSV format, and copy the exported file into CYBERQUEST monitoring folder;
- Access the CSV Processing template, provided with the CYBERQUEST Windows agent, found in the installation folder (C:\Program Files\CyberQuestAgent\templates). Use the template to process the exported files from HR system in the monitoring folder.

How-to · How to setup Windows Print Logs

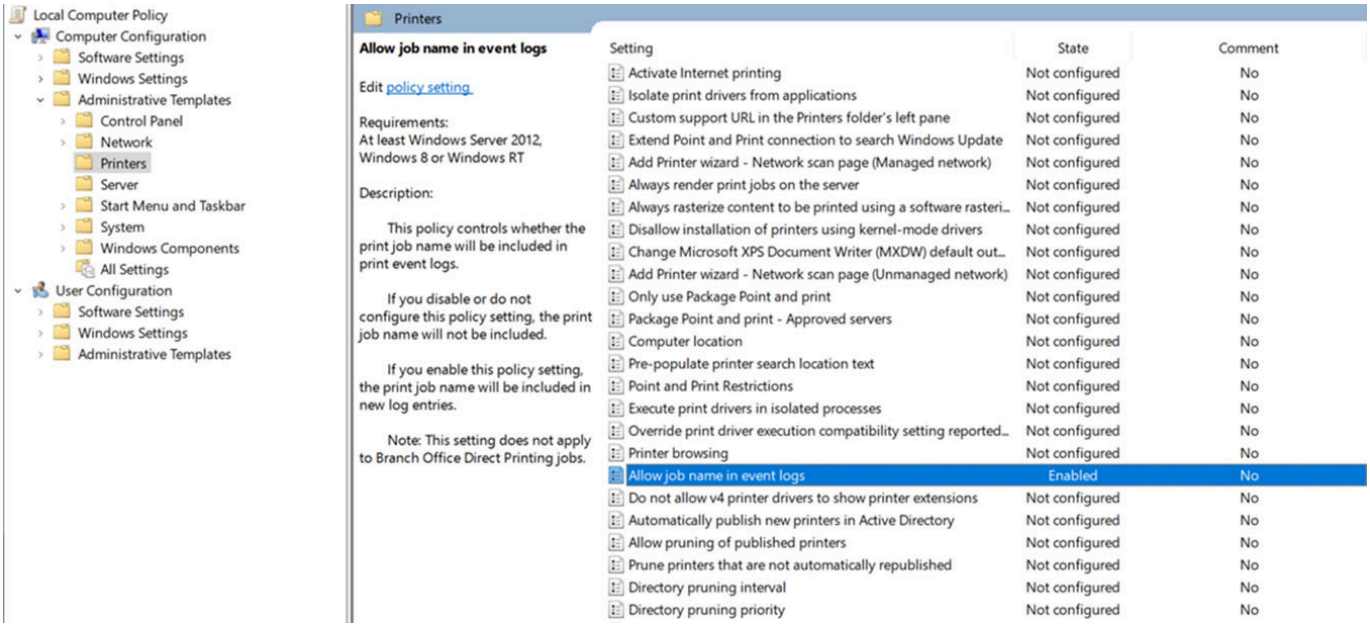
1. Run the script below (also contained in the **REG script print.reg** file):

```
Windows Registry Editor Version 5.00

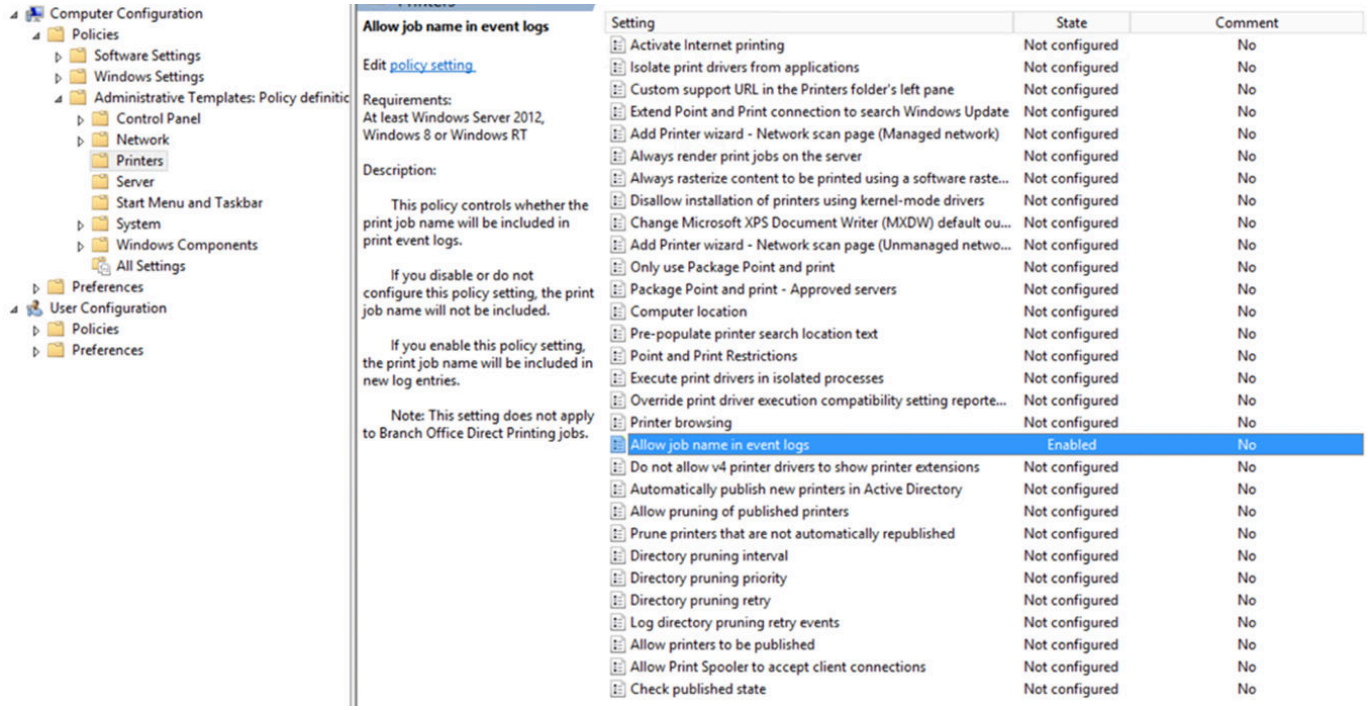
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Microsoft-Windows-PrintService/Operational]
" "=-
```

2. Enable **Allow job name** in event logs from:

A) **Edit group policy – Local policy**



B) **Group Policy Management – Domain policy**



How-to · How to Setup Windows Sysmon

System Monitor, commonly known as **Sysmon**, is a service and device driver for Windows systems that persists through system restarts once installed. Its purpose is to oversee and record system activities, storing this data in the Windows event log. It offers comprehensive insights into the initiation of processes, network connections, and modifications to the timestamps of file creation.

Please follow this steps to see how to setup WindowsSysmon:

1.The first step is to download the **Sysmon v15.11** from the official Microsoft website Sysmon v15.11 (https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon).

2.The second step is for the downloaded archive (Symon.zip) to be unzipped.

3.To install Sysmon, open CMD, navigate to the folder containing the unzipped archive using the command:

```
cd <folder name>
```

After which the following command will be executed:

```
sysmon64 -i
```

Once it is installed, Sysmon will start monitoring automatically. For more details related to installation and configuration, go to the Sysmon v15.11 (https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon).

In order for our Windows Agent to be able to send the logs to CYBERQUEST server, the following script must be run:

```
Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Microsoft-Windows-Sysmon/Operational] " "=-.
```

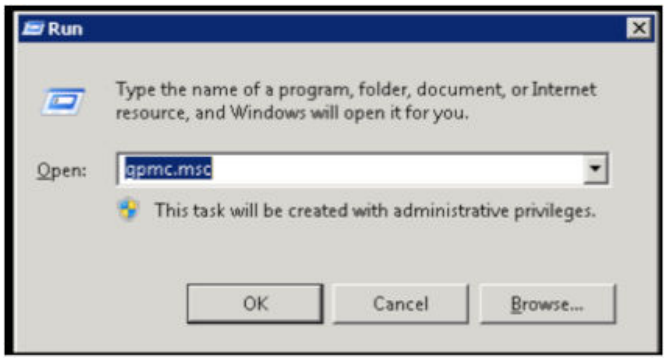
To view the events logs which are generated by **Sysmon**, you have to go to **EventViewer** and following this path: `Applications and Services Logs/Microsoft/Windows/Sysmon/Operational`

How-to · How to track changes made in Active Directory

Below are the steps you can take to enable auditing of Active Directory modifications using native processes:

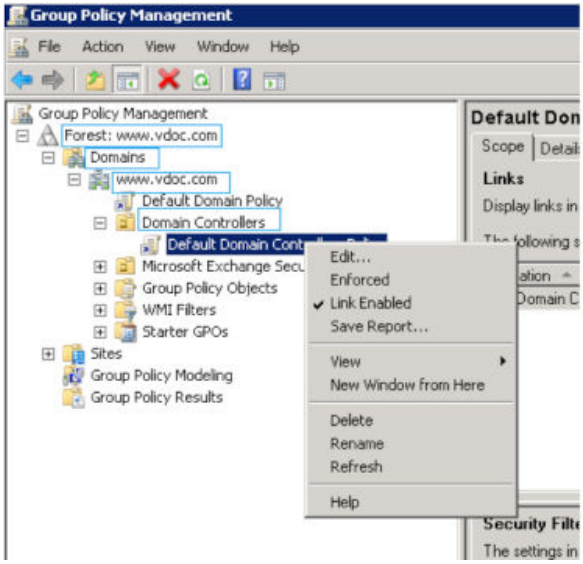
1. The configuration of Group Policy Audit Settings

Type the command **gpmc.msc** in order to open the **Group Policy Management Console**.



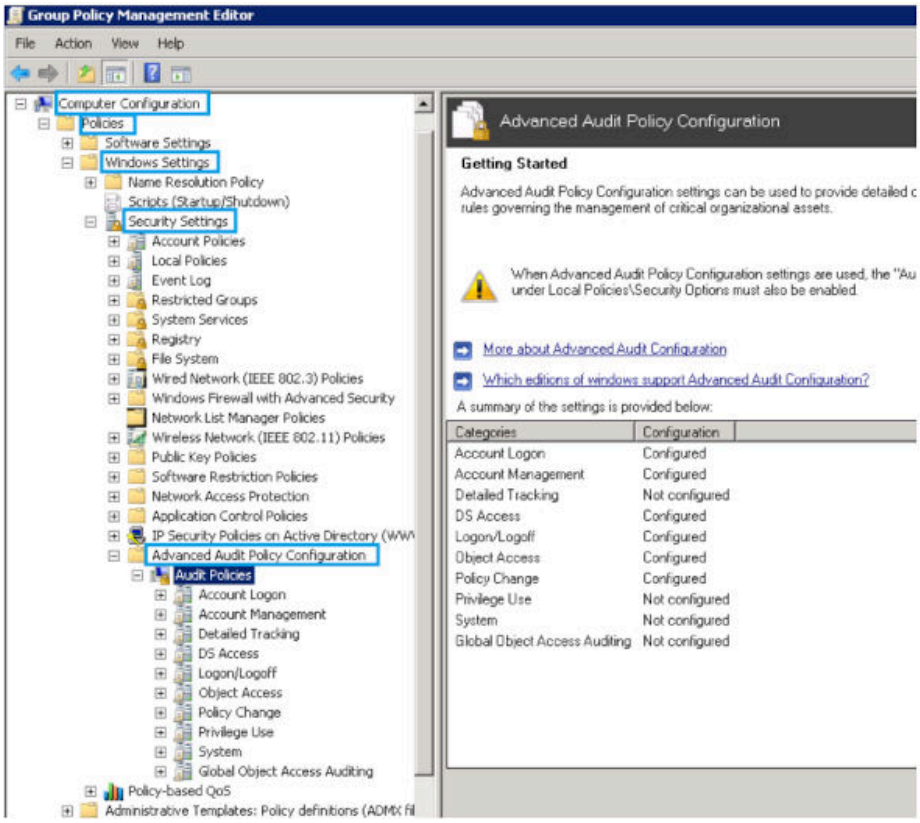
2. The Group Policy Management Console

Under **Group Policy Management**, select the **forest** domain you wish to choose and expand it further to navigate to the **Domain Controllers** > **Default Domain Controller Policy**, right click on it and select **Edit** to open the configuration window.



3. Advanced Audit Policy Configuration

Navigate to **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Advanced Audit Policy Configuration** > **Audit Policies** in the **Group Policy Management Editor**.



4. Configuring all the policies

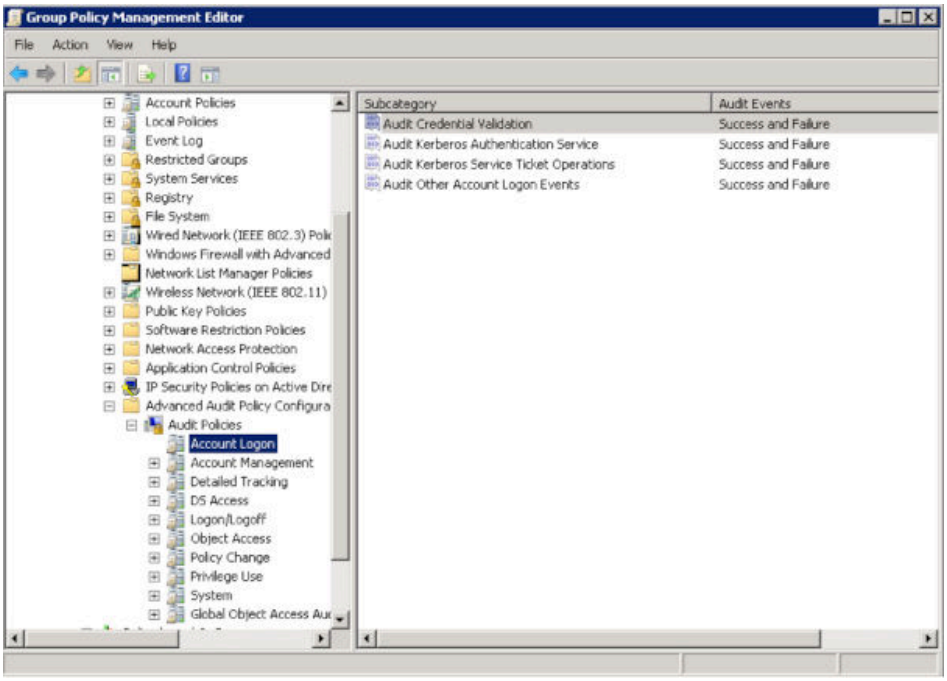
In order to configure all the policies, define the following categories and then configure them one after another:

- **Account Logon**
- **Account Management**
- **DS Access**
- **Logon/Logoff**
- **Object Access**

• **Policy Change**

5. Configuring all policies one by one

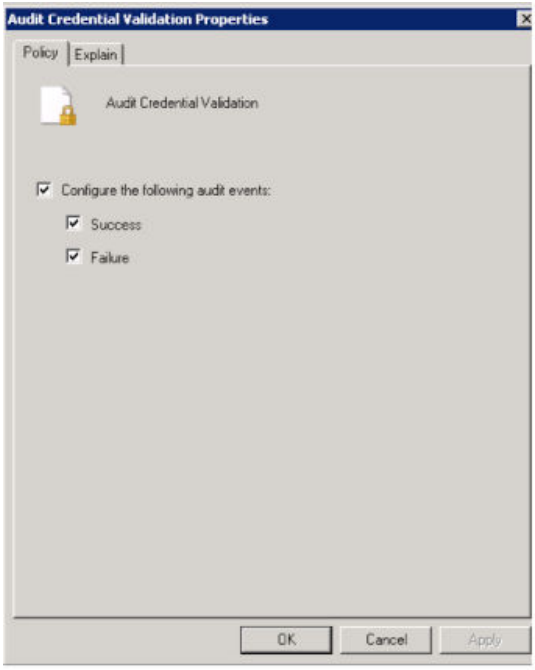
Click on the first policy - **Account Logon** and configure the audit events of its subcategories one after another.



6. Check both success and failure

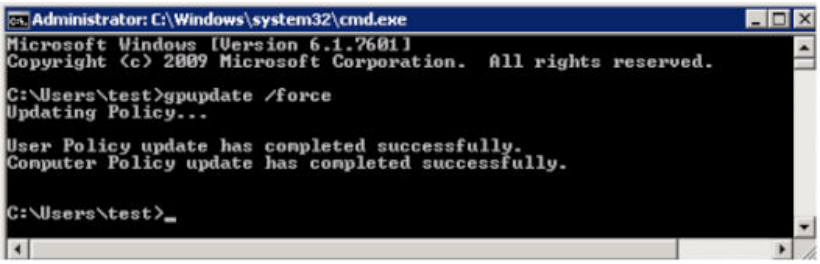
In the **Policy tab** of **Audit Credential Validation** window, simply check both the options - **success** and **failure** to audit the events and click **OK**.

Follow step 6 for all other Advanced Audit Policies listed above.



7. Updating the Group Policy

This can be done by executing the command: **gpupdate /force** in the command prompt.



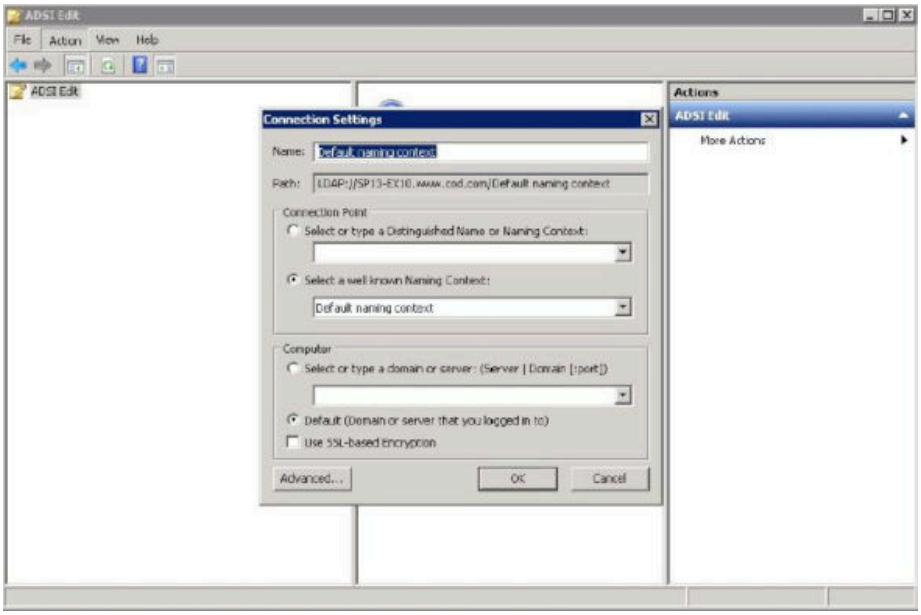
8. Use ADSIEdit.msc to Enable Auditing

A.Open **ADSI Edit** Console and select **Connect to** in order to view the Connection Settings.

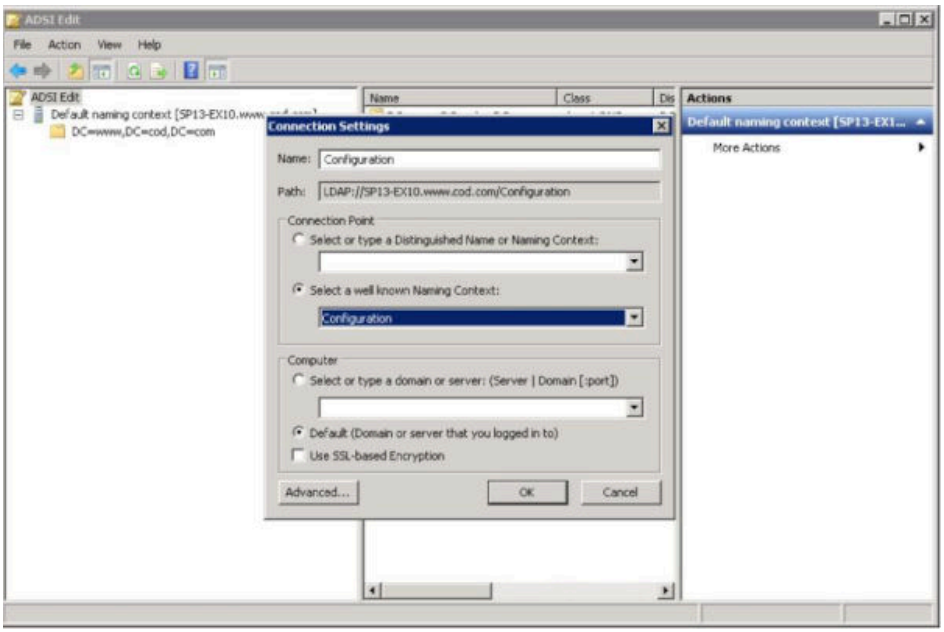
B.Next, establish connections with all four available naming contexts to turn on their auditing for:

- **Default Naming Context**
- **Configuration**
- **RootDSE**
- **Schema**

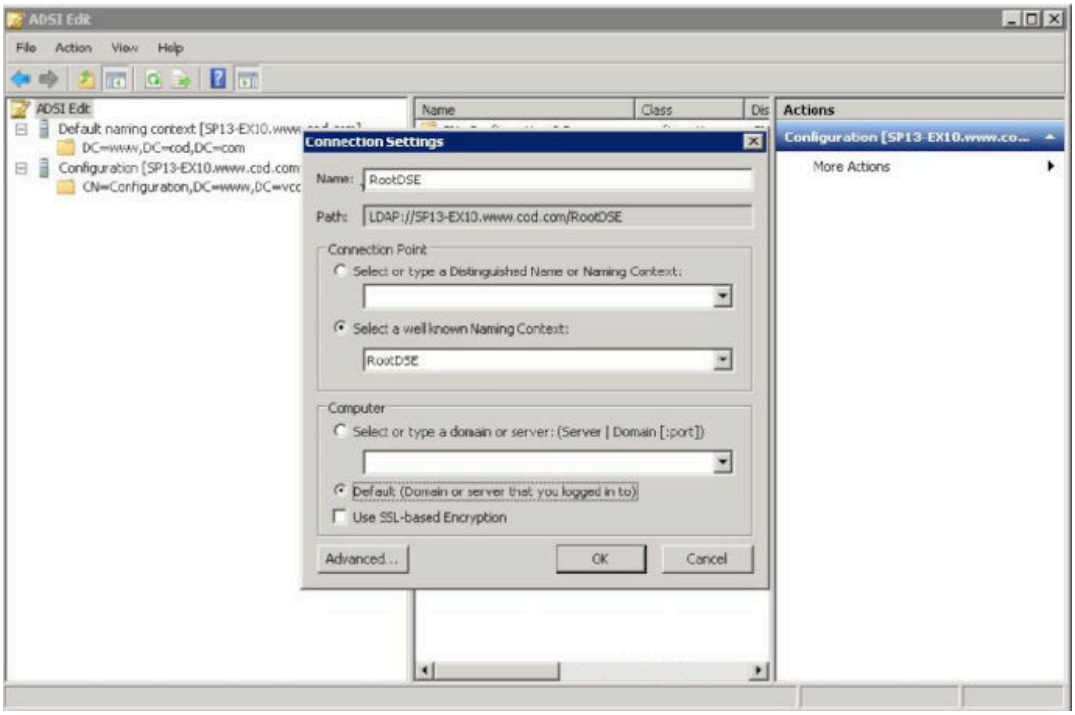
Then, proceed on to connect to the default naming context. Also, Right click on the node **ADSI Edit** and select **Connect To.**



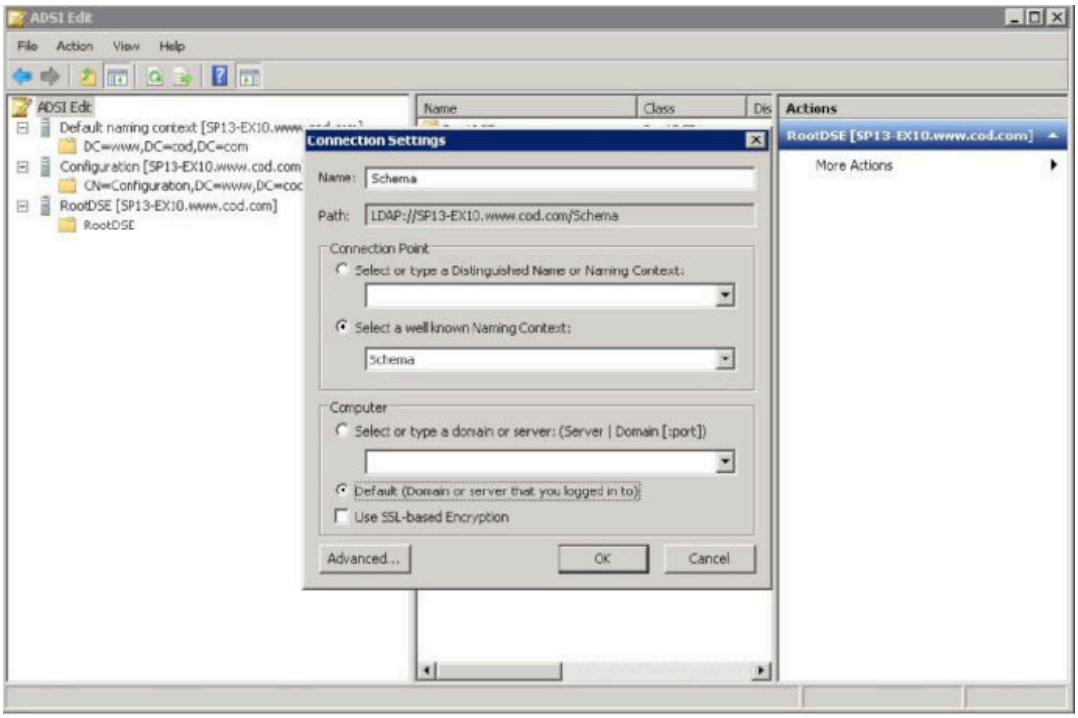
9. Configuring Connection Settings



10. Establishing connection with Root DSE

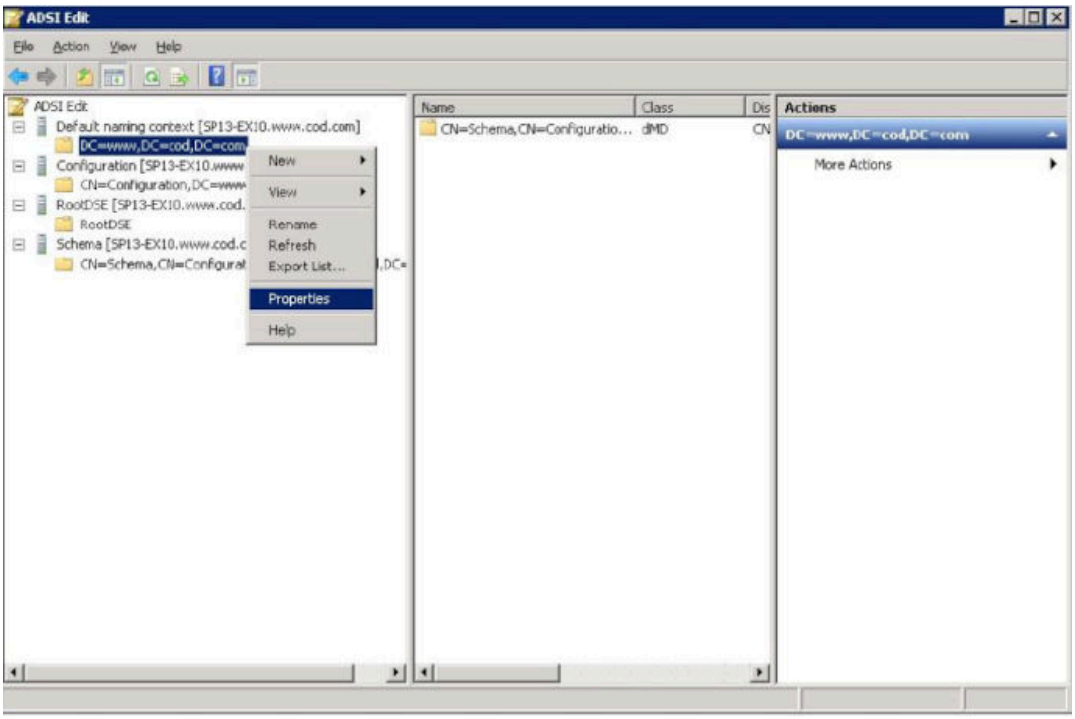


11. Connection Settings for Schema



12. Enabling the audit settings for all the four root nodes

For all the four root nodes of different naming contexts, enable the auditing settings.



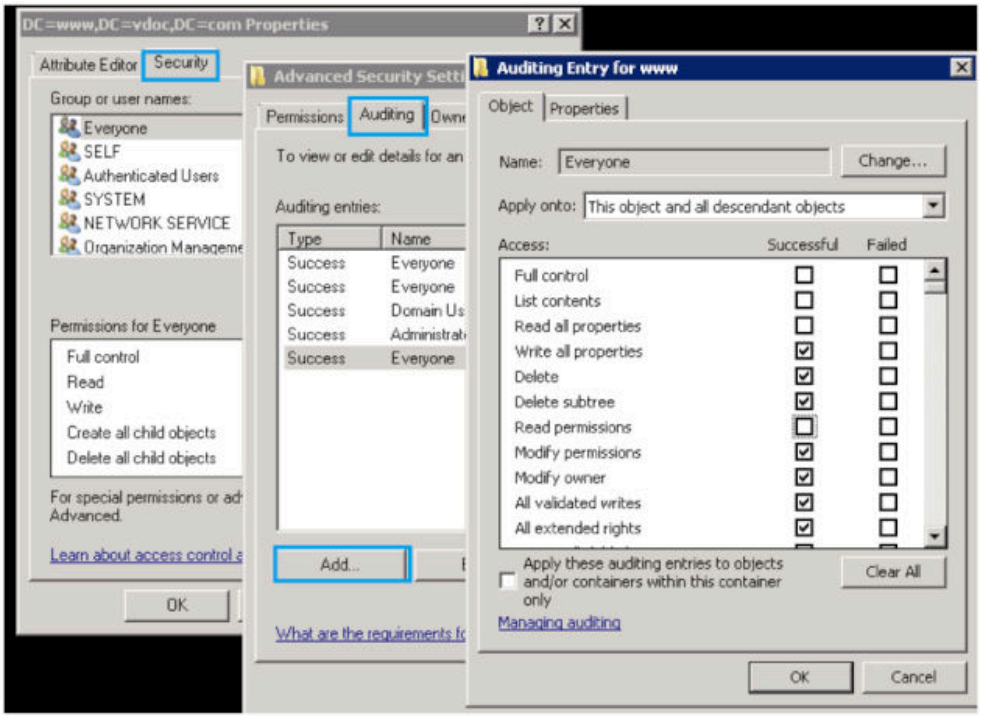
13. Managing Auditing Entry for your Domain

In the Domain Controller properties, navigate to the **Security** tab and click **Advanced**. This will open the **Advanced Security Settings**. Now, quickly navigate to the **Auditing** tab and click **Add** to open the **Auditing Entry** window. In the field **Name:** type “Everyone” and in the **Access** section, check all the boxes except the following four options:

- **Full Control**
- **List contents**
- **Read all properties**

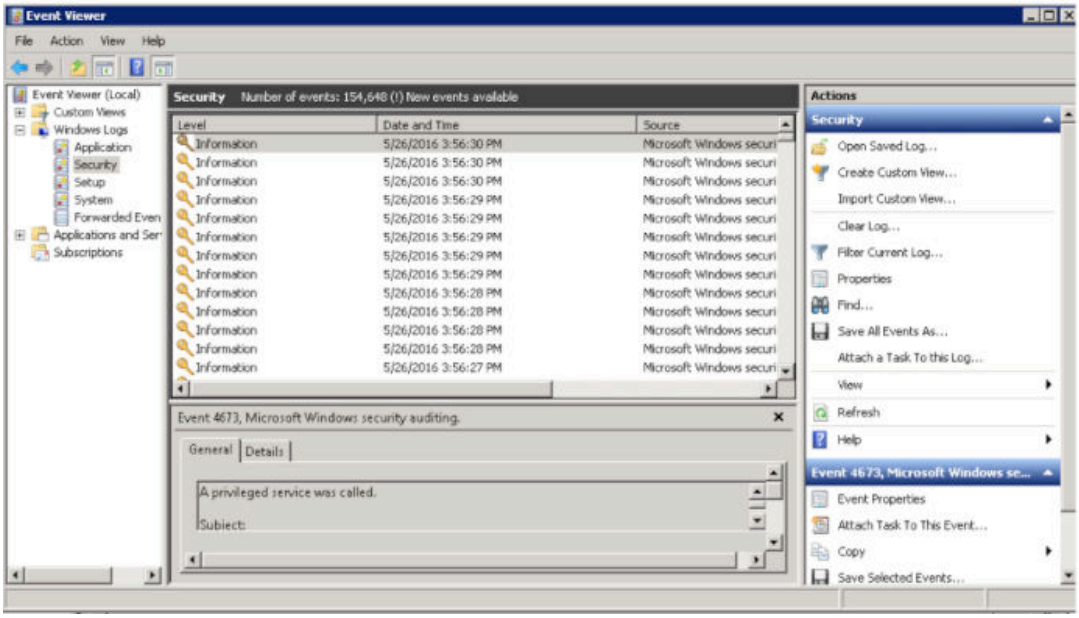
• **Read permissions**

In the **ADSI Edit**, repeat steps 3 and 4 in order to enable the auditing of the remaining root nodes.



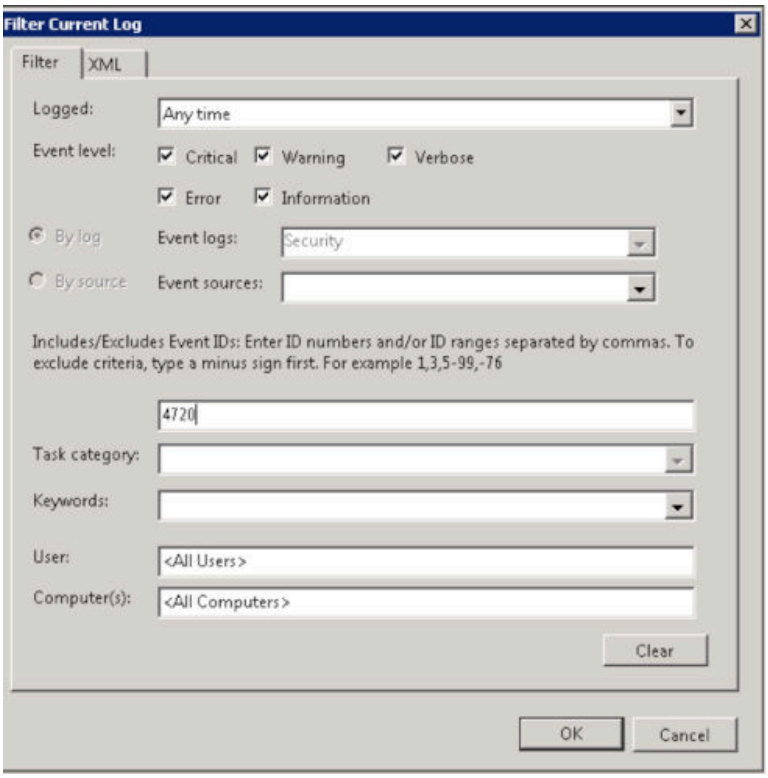
14. Filtering the Security Event Log

In the **Event Viewer**, navigate to **Windows Logs** and select **Security**. Then, simply click **Filter Current Log**.



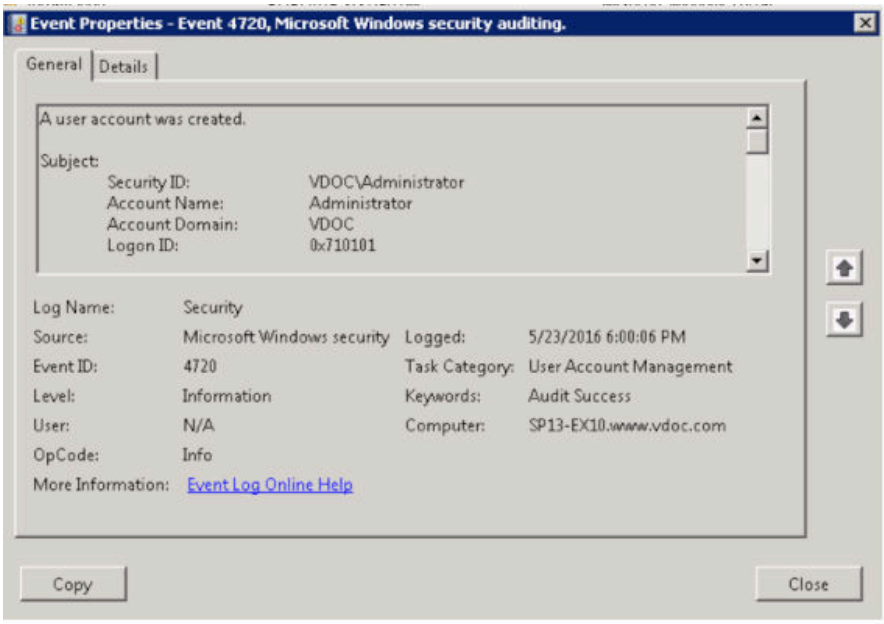
15. Search by Event ID

In the **Filter Current Log** window, simply enter the particular **Event ID** and carry out the search operation.



16. Open Event Properties to see further details.

To know more about any particular event, simply double click on it to see further details.



17. Here is a list of other relevant Event IDs

For many users, manual auditing can be both time consuming and unreliable, as does not generate instant alerts and reports for Active Directory changes.

It is therefore recommended that you opt for an automated Active Directory auditing solution. One such solution, LepideAuditor for Active Directory, that enables users to pro-actively track, alert and report on changes being made to Active Directory.

Event ID	Evnt ID Description	Event ID	Evnt ID Description
4661	A handle to an object was requested	4730	A security-enabled global group was deleted.
4662	An operation was performed on an object.	4731	A security-enabled local group was created.
5139	A directory service object was moved.	4732	A member was added to a security-enabled local group.
5136	A directory service object was modified.	4733	A member was removed from a security-enabled local group.
5137	A directory service object was created.	4734	A security-enabled local group was deleted.
5138	A directory service object was undeleted	4735	A security-enabled local group was changed.
5139	A directory service object was moved	4737	A security-enabled global group was changed.
5141	A directory service object was deleted.	4754	A security-enabled universal group was created.
4720	A user account was created.	4755	A security-enabled universal group was changed.
4722	A user account was enabled.	4756	A member was added to a security-enabled universal group.
4723	An attempt was made to change an account's password.	4757	A member was removed from a security-enabled universal group.
4724	An attempt was made to reset an accounts password.	4758	A security-enabled universal group was deleted.
4725	A user account was disabled.	4764	A group type was changed.
4726	A user account was deleted.	4744	A security-disabled local group was created.
4738	A user account was changed.	4745	A security-disabled local group was changed.
4740	A user account was locked out.	4746	A member was added to a security-disabled local group.
4767	A user account was unlocked.	4747	A member was removed from a security-disabled local group.
4780	The ACL was set on accounts which are members of administrators groups.	4748	A security-disabled local group was deleted.
4781	The name of an account was changed.	4749	A security-disabled global group was created.
4794	An attempt was made to set the Directory Services Restore Mode administrator password	4750	A security-disabled global group was changed.
5376	Credential Manager credentials were backed up.	4751	A member was added to a security-disabled global group.
5377	Credential Manager credentials were restored from a backup.	4752	A member was removed from a security-disabled global group.
4741	A computer account was created.	4753	A security-disabled global group was deleted.
4742	A computer account was changed.	4759	A security-disabled universal group was created.
4743	A computer account was deleted.	4760	A security-disabled universal group was changed.
4727	A security-enabled global group was created.	4761	A member was added to a security-disabled universal group.
4728	A member was added to a security-enabled global group.	4762	A member was removed from a security-disabled universal group.
4729	A member was removed from a security-enabled global group.	4763	A security-disabled universal group was deleted.

How-to · OSSEC Configuration

1.**Configure OSSEC:** Edit the configuration file ossec.conf:

```
sudo nano /var/ossec/etc/ossec.conf

  <client>

    <server-ip> IP SERVER OSSEC </server-ip>

  </client>


  <syslog_output>

    <server>IP CYBERQUEST</server>

    <port>5140</port>

    <format>json</format>

    <level>5</level>

  </syslog_output>
```

```
<global>

    <allow_list>127.0.0.1</allow_list>

    <allow_list>::1</allow_list>

    <allow_list>localhost.localdomain</allow_list>

    <allow_list>IP DNS</allow_list>

    <allow_list>IP DNS</allow_list>

    <allow_list>IP Cyberquest</allow_list>

</global>
```

2.**Enabling Syslog Logging on the Server**

```
/var/ossec/bin/ossec-control enable client-syslog
```

```
/var/ossec/bin/ossec-control restart
```

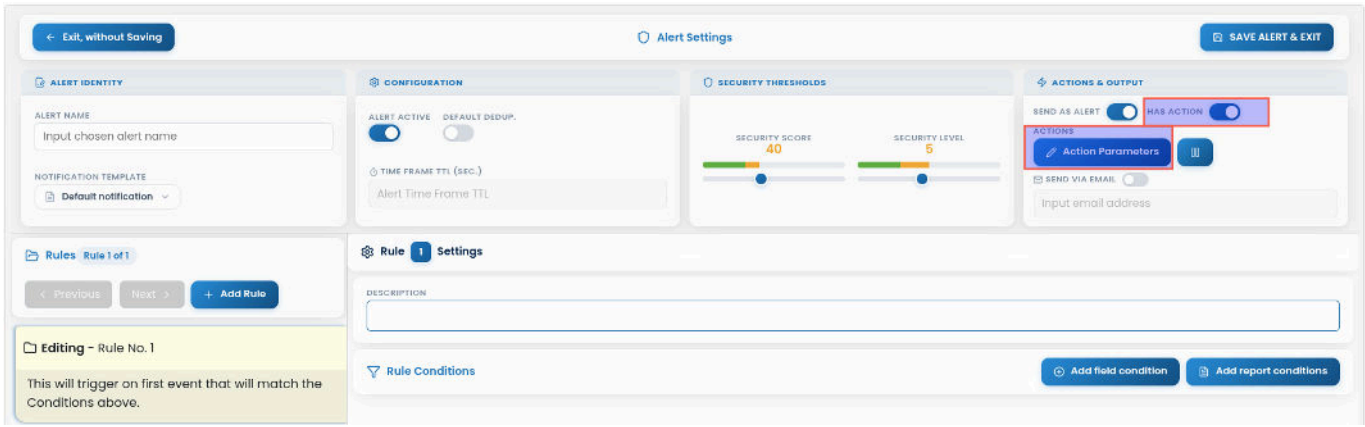
Operations · How to activate automatic Actions in Realtime Alerts

To use predefined automatic actions, first create a new alert or open/edit an existing scenario or alert.

For instructions on creating a new alert, please refer to the provided link: How to create new alerts

To access Action Parameters, open the **ALERT SETTINGS** menu by navigating to *Settings > Alerts > Realtime*. The **Alerts** customization page will open within the **Alerts** module interface.

When creating or editing an alert, the **Has Action** checkbox will be available:



Press



to open the Action Parameters window, which includes a drop-down list of automated actions and provides access to the Script Editor for creating a custom script.



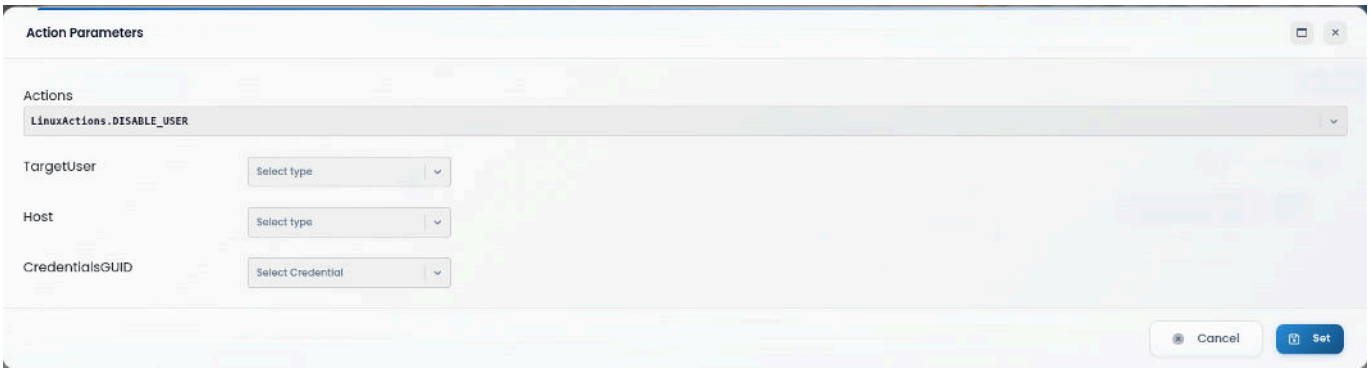
Selecting a specific action (e.g., disabling a Linux user account) enables an automated response scenario. These actions can include enabling or disabling user accounts, sending notifications via email or messenger, and more.

An action is executed in response to alerts triggered by specific event conditions.

The following predefined automated actions are currently available:

1.LinuxActions.DISABLE_USER

This automated action disables or removes specified Linux user accounts from the target host, based on the defined parameters:



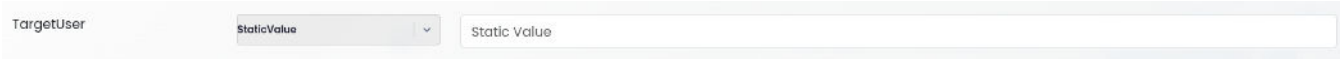
- **Target User** - Specifies the user account to be disabled.
- **Host** - Defines the system where the action is to be applied.
- **CredentialsGUID** Specifies the credentials used by the CYBERQUEST server to perform the action.

This action requires root password to execute.

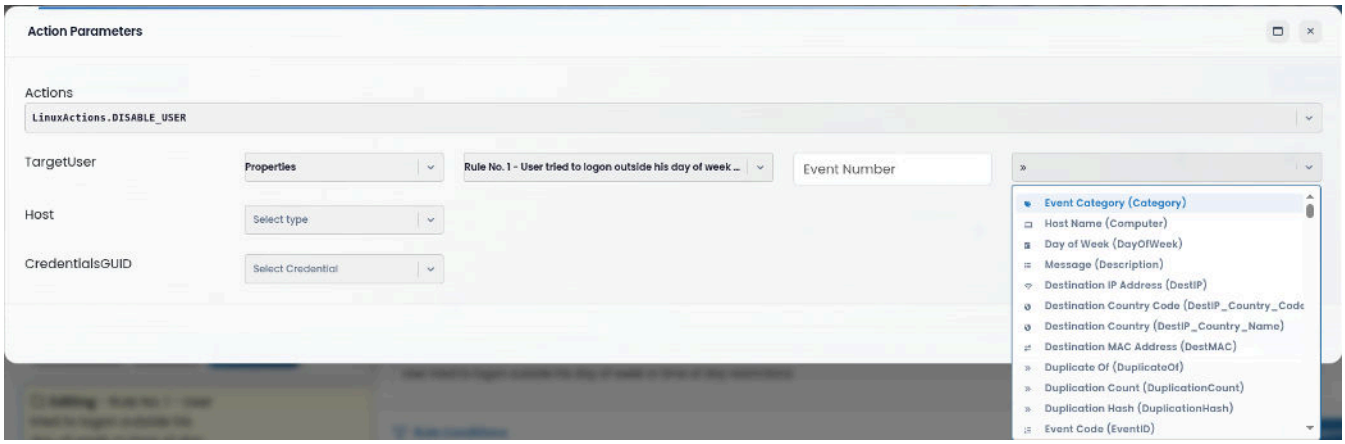
Upon execution, the specified user will be removed from the target system and will no longer be able to authenticate or log in.

Target User:

- Static Value - A fixed username can be provided directly in the field. The specified user will be disabled based on this static input:



- Properties - Allows dynamic selection of the user based on event data. Use the *UserName* field from a specified rule and event index to determine which user will be disabled:



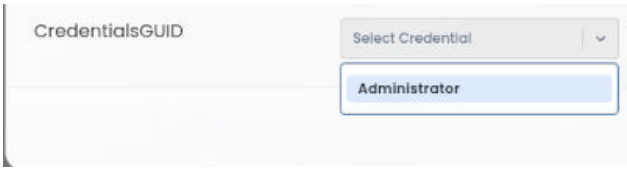
Host:

- Specifies the target system where the user account will be disabled. This can be the host from which the event originated or a specific machine (e.g., `DC09`)



CredentialsGUID:

Specifies the credentials used by the CYBERQUEST server to execute the action. The appropriate credential (e.g., `AgentWindows`) is selected from a predefined list:



2.LinuxActions.ENABLE_USER

This action activates or restores a specific Linux user account, allowing the user to log in again. It operates based on the following parameters:

- **Target User** - Specifies the user account to be enabled
- **Host** - Indicates the host where the account will be reactivated
- **CredentialsGUID** - Defines the credentials used to perform the action

This action requires root password to execute.

Target User:

- **Static Value** - A fixed username can be provided directly in the Static Value field to specify the user account to be enabled.
- **Properties** - A dynamic selection that allows choosing a username from a specific rule and event instance using the *UserName* field. This enables the action to target users identified at runtime.

Host:

- Specifies the target system where the action will be executed. This can be the originating host or a specific system like a domain controller (e.g., `DC09`).

CredentialsGUID:

- Indicates which stored credentials from the CYBERQUEST server are used to perform the action. The credentials are selected from an available list (e.g., `AgentWindows`).

3.LinuxActions.EXPIRE_USER_PASSWORD

This action enforces password expiration for a specified Linux user, preventing further logins using the current password. Configuration requires the following parameters:

- **Target User** - The user whose password will be expired
- **Host** - The system where the action is applied
- **CredentialsGUID** - The credentials used to perform the operation

Execution can be carried out by a group administrator or a user with sufficient privileges; root access is not mandatory.

Target User:

- Static Value - Enter a specific username whose password should be expired.
- Properties - Dynamic values can be applied by selecting the rule and event number from the list. For example, the *UserName* field can be used to dynamically identify the target user.

Host:

- Specifies the target system where the action will be executed. This can be the originating host or a specific system like a domain controller (e.g., `DC09`).

CredentialsGUID:

- Select the credentials (e.g., `AgentWindows`) from the CYBERQUEST server that will be used to execute the password expiration action.

4.LinuxActions.DISABLE_PASSWORD_EXPIRE

This action disables password expiration for a specified Linux user, allowing the user to log in without being restricted by an expired password. The action is performed based on the following parameters:

- **Target User** - The Linux user account for which password expiration is to be disabled.
- **Host** - The system where the action will be executed.
- **CredentialsGUID** - The credentials used by CYBERQUEST to perform the action on the target host.

Could be done by group administrator.

Target User:

- Static Value - A fixed username can be specified directly. In this case, the user name is manually entered into the Static Value field.
- Properties - Dynamic values can be used by selecting a rule and event number from the list. For example, the `UserName` field can be referenced to dynamically identify the account for which password expiration should be disabled.

Host:

Specifies the target system where the action will be executed. This can be the originating host (where the triggering event occurred) or a designated system like a domain controller (e.g., `DC09`).

CredentialsGUID:

Indicates the credentials to be used by the CYBERQUEST server when executing the action. A credential entry (e.g., `AgentWindows`) must be selected from the predefined list available in the system.

5.Notifications Email/ Teams/Slack/Jira

These actions trigger automatic notifications through selected communication channels, including Email, Microsoft Teams, Slack, or Jira, based on the alert conditions defined.



The custom message defined by the user, which will be delivered when the alert is triggered by a matching event. This message typically includes context about the detected risk or condition.

6.PlayBooks.RUN_PLAYBOOK

This action triggers the execution of a defined playbook in response to the alert instance. When the alert conditions are met, the associated playbook is automatically initiated, enabling a structured and automated response workflow. Playbooks may include a series of predefined tasks, actions, or decisions designed to handle specific security events or operational scenarios.



AlertSecurityThreshold - Sets a static numeric value to define the security impact level of the alert.

Run Playbook - Selects a playbook from the list of available entries defined in the Playbooks module to be executed when the alert is triggered.

7.LinuxActions.MANIPULATE_SERVICE

This action performs operations on a specified Linux service - starting, stopping, or restarting it - based on defined parameters.

ServiceName - Identifies the name of the Linux service to be manipulated

Action - Specifies the type of service operation (start, stop, restart)

Host - Indicates the host on which the service operation will be executed

CredentialsGUID - Indicates the credentials to be used by the CYBERQUEST server when executing the action. A credential entry (e.g., `AgentWindows`) must be selected from the predefined list available in the system.

This action requires root password access to execute successfully.

ServiceName:

- **Static Value** - A fixed service name can be entered directly (e.g., `sshd`, `nginx`).
- **Properties** - Enables dynamic selection of the service name from a rule and event instance, allowing flexible automation based on event data.

Action:

- **Static Value** - Allows selecting the desired operation from a predefined list (e.g., `start`, `stop`, `restart`).
- **Properties** - Enables dynamic selection of the operation by referencing a specific field from the triggering event or rule, allowing the action to adapt based on runtime data.

Host:

- Specifies the target system where the action will be executed. This can be the originating host (where the triggering event occurred) or a designated system like a domain controller (e.g., `DC09`).

CredentialsGUID:

- Indicates the stored credentials from the CYBERQUEST server used to authenticate and execute the service command. Credentials are selected from a list (e.g., `AgentLinuxRoot`).

8.LinuxActions.BLOCK_IP_ADDRESS

This action blocks a specific IP address on a designated Linux host using defined parameters. It is typically used to prevent communication from potentially malicious sources.

IpAddress - Specifies the IP address to be blocked.

Host - Indicates the host on which the block action will be applied.

CredentialsGUID - Defines the credentials used to perform the action.

This action requires root access to execute.

IpAddress:

- **Static Value** - A specific IP address can be manually entered to apply a fixed blocking rule.
- **Properties** - Enables dynamic selection of the IP address from a rule and event instance (e.g., using the *SourceIP* field) to block addresses identified at runtime.

Host:

- Specifies the Linux host where the IP address will be blocked. This can be the host from which the triggering event was collected or a designated target system (e.g., `Server02`).

CredentialsGUID:

- Indicates which stored credentials from the CYBERQUEST server will be used to execute the command. Select from the available list (e.g., `AgentLinux`).

9.LinuxActions.REMOVE_BLOCK_IP_ADDRESS

This action removes a previously applied block on a specific IP address on a designated Linux host, based on the provided parameters.

- **IpAddress** - Specifies the IP address to unblock.
- **Host** - Indicates the host where the block removal will be performed.
- **CredentialsGUID** - Defines the credentials used to execute the action.

IpAddress:

- **Static Value** - A fixed IP address can be entered manually to specify which address to unblock.
- **Properties** - Allows dynamic selection of the IP address from a rule and event instance (e.g., *SourceIP* field), enabling unblock actions based on real-time event data.

Host:

- Specifies the Linux host where the block on the IP address will be removed. This can be the original host or another target system.

CredentialsGUID:

- Indicates which stored credentials from the CYBERQUEST server will be used to run the unblock command. Choose from the available list (e.g., `AgentLinux`).

10.LinuxActions.KILL_PROCESS_BY_PID

This action terminates a specific process on a Linux host using its Process ID (PID), based on the provided parameters.

- **PID** - Specifies the Process ID of the process to be terminated.
- **Host** - Indicates the host where the process termination will be executed.
- **CredentialsGUID** - Defines the credentials used to perform the action.

Root access is required to execute this action.

PID:

- **Static Value** - A fixed Process ID can be entered manually to specify which process to kill.
- **Properties** - Enables dynamic selection of the PID from a rule and event instance, allowing process termination based on real-time event data.

Host:

- Specifies the Linux host where the process termination will be carried out. This can be the originating host or a designated system.

CredentialsGUID:

- Indicates which stored credentials from the CYBERQUEST server are used to perform the kill operation. Select from the available list (e.g., `AgentLinux`).

11.LinuxActions.KILL_PROCESS_BY_NAME

This action terminates a Linux process based on its name, using the following parameters:

- **ProcessName** - Specifies the name of the process to be terminated.
- **Host** - Indicates the host where the process will be killed.
- **CredentialsGUID** - Defines the credentials used to perform the action.

ProcessName:

- **Static Value** - A fixed process name can be entered directly to specify which process to terminate.
- **Properties** - Supports dynamic selection of the process name from a rule and event instance, enabling process termination based on real-time event data.

Host:

- Specifies the target system where the action will be executed. This can be the originating host or another designated system.

CredentialsGUID:

- Indicates which stored credentials from the CYBERQUEST server are used to execute the action. Credentials are selected from the available list.

12.LinuxActions.CQ_SERVICES_STATUS

This action checks the status of CyberQuest services on a specified host, using the following parameters:

- **Host** - Specifies the target system where the service status check will be performed.
- **CredentialsGUID** - Defines the credentials used to execute the status query.

Host:

- Selects the system on which the CyberQuest service status will be checked. This can be the originating host or another designated system.

CredentialsGUID:

- Indicates which stored credentials from the CYBERQUEST server are used to perform the action, selected from the available list.

13.LinuxActions.VALIDATE_CERTIFICATE

This action validates SSL/TLS certificates on a specified host using the following parameter:

- **Host** - Specifies the target system where the certificate validation will be performed.

Host:

- Selects the system on which the certificate validation process will be executed. This can be the originating host or another designated system.

14.LinuxActions.CHECK_IF_OS_IS_WINDOWS

This action checks whether the specified host is running a Windows operating system, based on the following parameter:

- **Host** - Specifies the target system to verify the OS type.

Host:

- Selects the system on which the OS check will be performed. This can be the originating host or another designated system.

15.WindowsActions.DISABLE_USER

This action disables a specific Windows user account on the target host, based on the following parameters:

- **TargetUser** - Specifies the user account to be disabled
- **Host** - Indicates the system where the user account will be disabled
- **CredentialsGUID** - Defines the credentials used to perform the action

TargetUser:

- **Static Value** - A fixed username can be provided directly to specify the user account to disable.
- **Properties** - Supports dynamic selection of the user account from rule and event data (*e.g.,* `UserName` *field*), enabling the action to target users identified in real time.

Host:

- **Static Value** - A fixed host name or IP address can be set as the target system.
- **Properties** - Allows dynamic selection of the host from rule and event information where the action will be executed.

CredentialsGUID:

- Specifies the stored credentials used by CYBERQUEST to perform the action, selected from an available list.

16.WindowsActions.ENABLE_USER

This action enables a specific Windows user account on the target host, based on the following parameters:

- **TargetUser** - Specifies the user account to be enabled
- **Host** - Indicates the system where the user account will be enabled
- **CredentialsGUID** - Defines the credentials used to perform the action

TargetUser:

- **Static Value** - A fixed username can be provided directly to specify the user account to enable.
- **Properties** - Supports dynamic selection of the user account from rule and event data (*e.g.,* `UserName` *field*), enabling the action to target users identified in real time.

Host:

- **Static Value** - A fixed host name or IP address can be set as the target system.
- **Properties** - Allows dynamic selection of the host from rule and event information where the action will be executed.

CredentialsGUID:

- Specifies the stored credentials used by CYBERQUEST to perform the action, selected from an available list.

17.WindowsActions.START_SERVICE

This action starts a specified Windows service on the target system, based on the following parameters:

- **TargetService** - Identifies the service to be started
- **Host** - Indicates the system where the service should be started
- **CredentialsGUID** - Defines the credentials used to execute the action

TargetService:

- **Static Value** - A specific service name can be provided directly (e.g., `Spooler`) to be started.
- **Properties** - Allows dynamic identification of the service name using rule and event fields, enabling contextual response.

Host:

- **Static Value** - A predefined hostname or IP address can be manually entered.
- **Properties** - Allows dynamic selection of the host from rule and event information where the action will be executed.

CredentialsGUID:

- Specifies which stored credentials from CYBERQUEST are used to start the service. The credentials are selected from a predefined list.

18.WindowsActions.STOP_SERVICE

This action stops a specified Windows service on the target system using the parameters below:

- **TargetService** - Specifies the service to be stopped
- **Host** - Indicates the system where the service is running
- **CredentialsGUID** - Defines the credentials used to execute the action

TargetService:

- **Static Value** - Enter the exact name of the service to be stopped (e.g., `Spooler`).
- **Properties** - Dynamically determines the service name from event context fields, allowing context-aware service control.

Host:

- **Static Value** - Manually specify a fixed host (hostname or IP).
- **Properties** - Allows dynamic selection of the host from rule and event information where the action will be executed.

CredentialsGUID:

- Selects the credential from the CYBERQUEST server to authorize the action. Credentials are chosen from a predefined list.

19.WindowsActions.RESTART_SERVICE

This action restarts a specific Windows service on a designated host, based on the following parameters:

- **TargetService** - Defines the Windows service that will be restarted
- **Host** - Specifies the system where the service restart will be executed
- **CredentialsGUID** - Indicates the credentials used to authenticate and perform the action

TargetService:

- **Static Value** - A fixed service name can be entered directly in the Static Value field to identify the service to restart.
- **Properties** - Allows dynamic selection of the service name from a rule and event instance, making the action responsive to contextual event data.

Host:

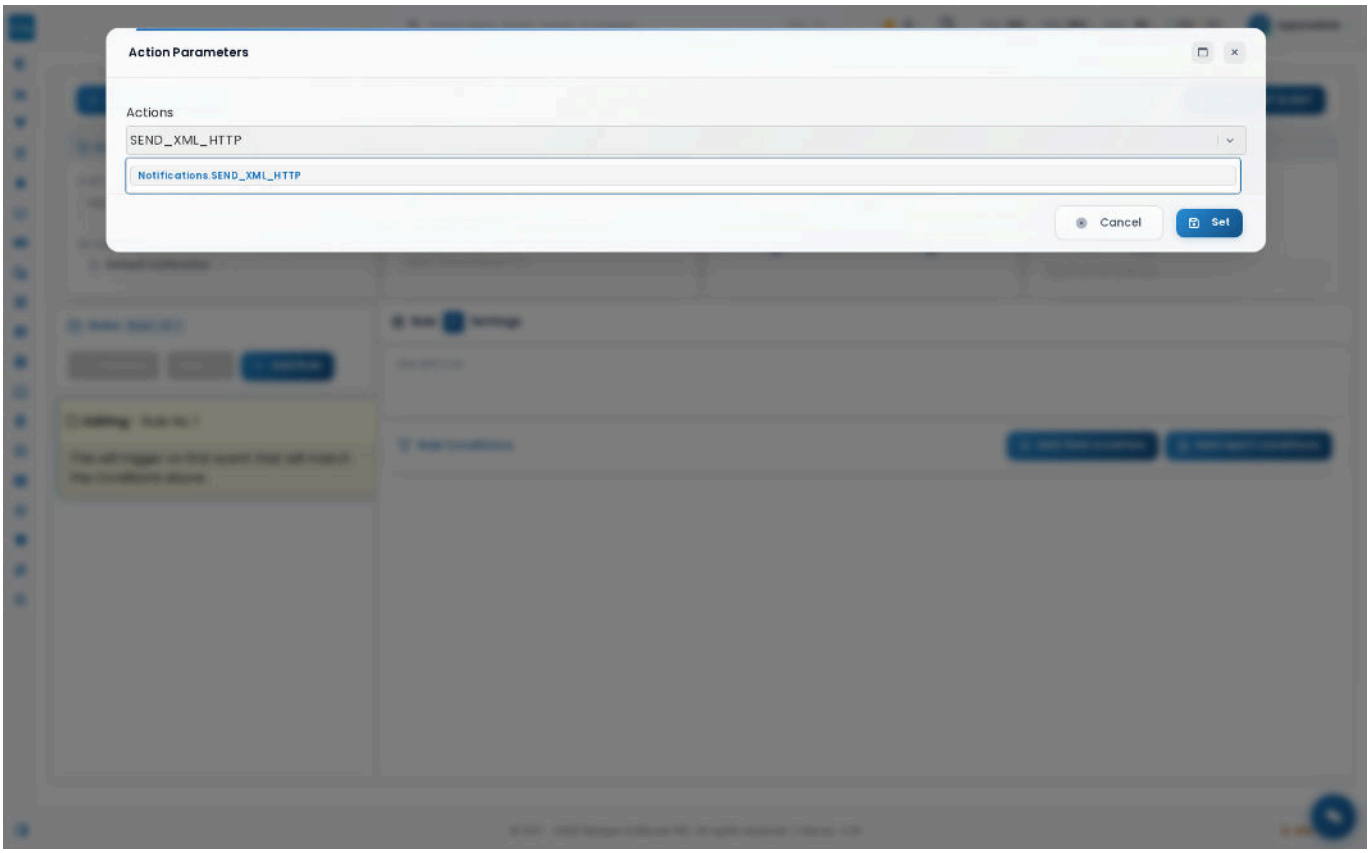
- **Static Value** - A specific host name can be entered directly to identify where the service will be restarted.
- **Properties** - Dynamically retrieves the host from the rule or event data, targeting the system that triggered the alert.

CredentialsGUID:

- Specifies which stored credentials from the CYBERQUEST server will be used to perform the operation. The appropriate credential (e.g., *AgentWindows*) is selected from a predefined list.

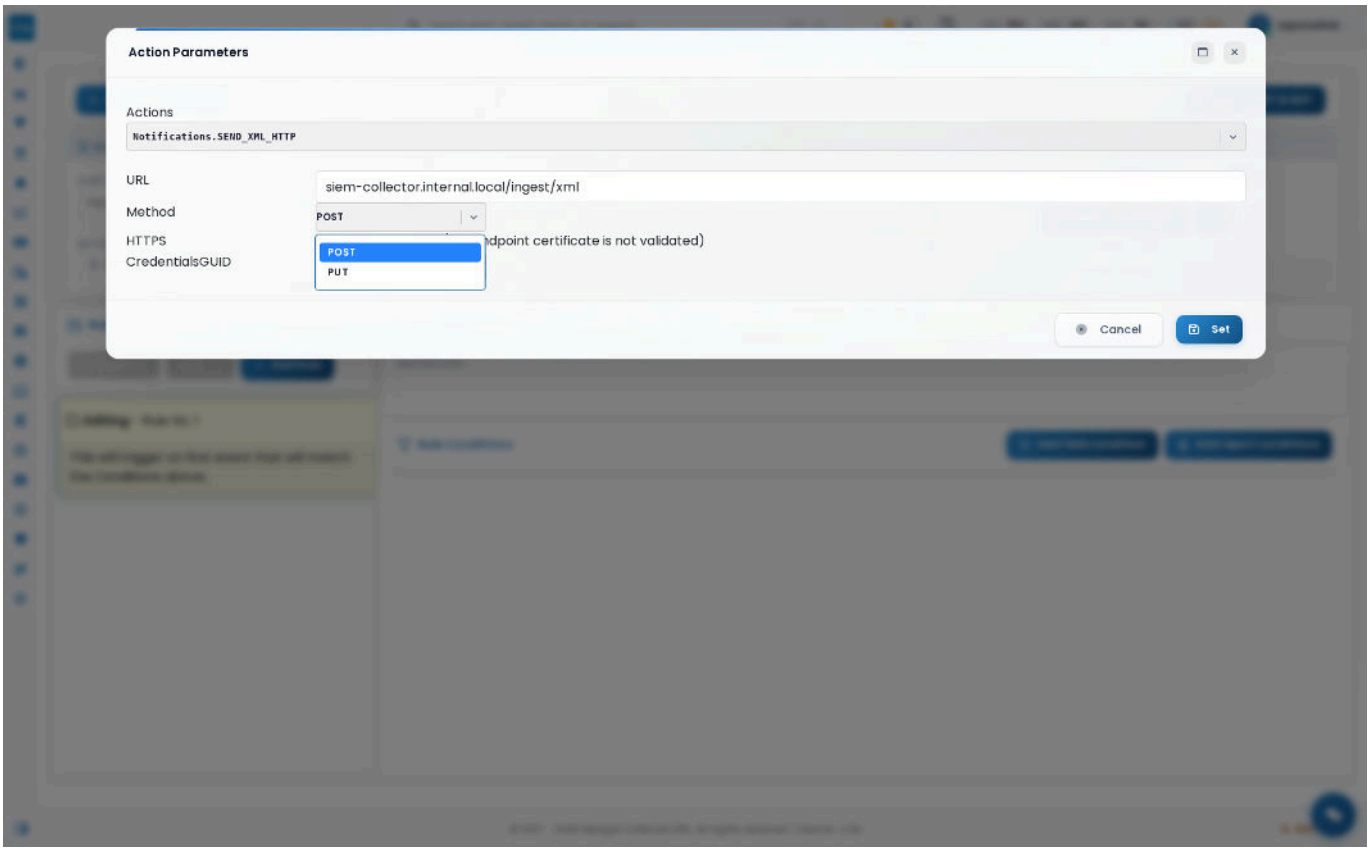
20.Notifications.SEND_XML_HTTP

This action sends the triggering alert as an XML document to an external endpoint, over HTTP or HTTPS. It is available in the same action list as the other notification channels (Email, Teams, Slack, Jira), and is used when the receiving system expects an XML payload delivered over a plain HTTP(S) request rather than email or a chat webhook.

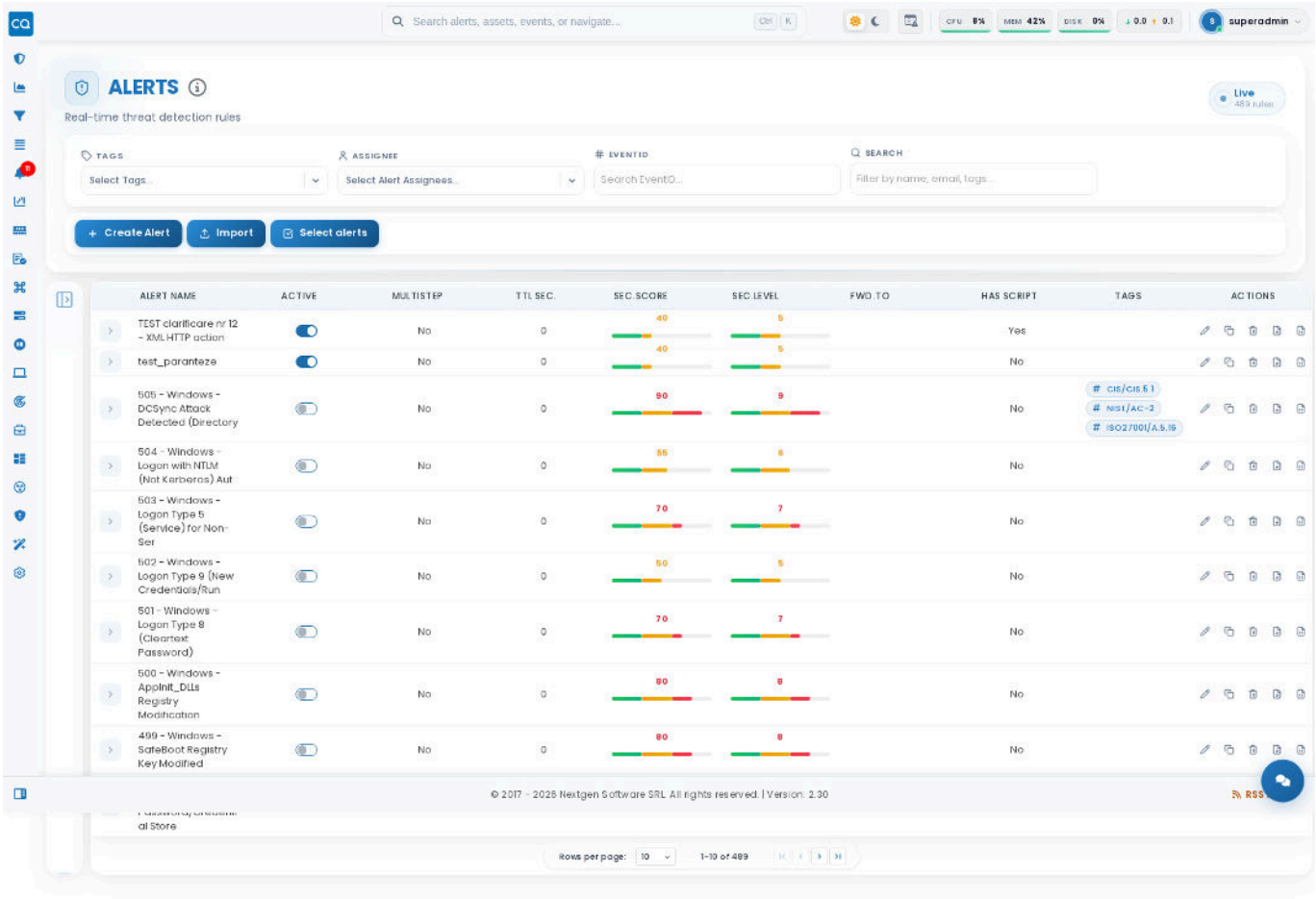


Selecting the action exposes four parameters:

- **URL** - The destination address for the XML document (the host and path, without a scheme).
- **Method** - The HTTP method used to send the file. Only the methods that carry a request body are offered.
- **HTTPS** - A checkbox that sends the request over an encrypted connection when enabled. The scheme is always derived from this checkbox, not from any scheme typed into the URL field.
- **CredentialsGUID** - An optional credential from the CYBERQUEST credentials vault, for endpoints that require authentication.

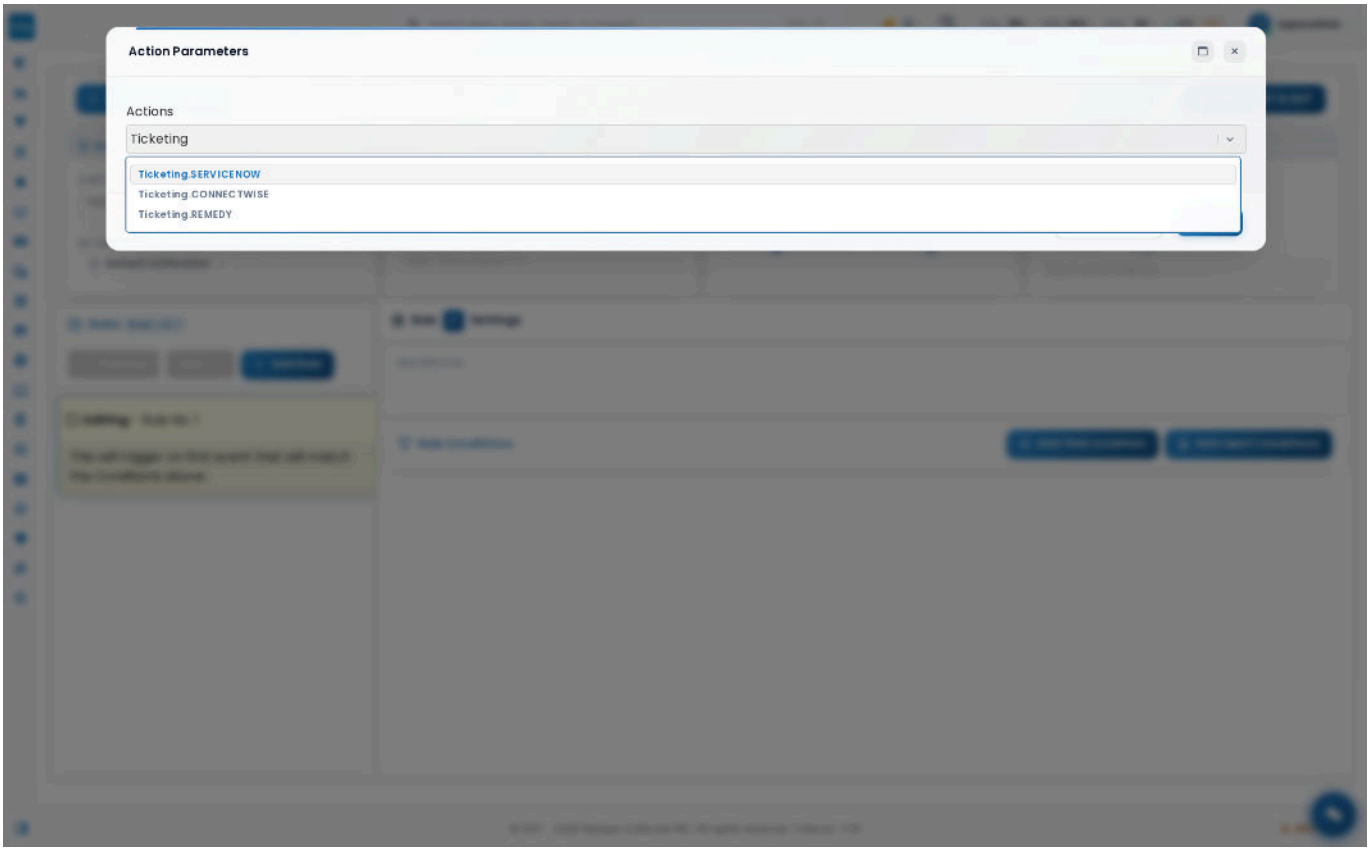


Once saved as part of an alert rule, the action is applied every time the rule triggers:



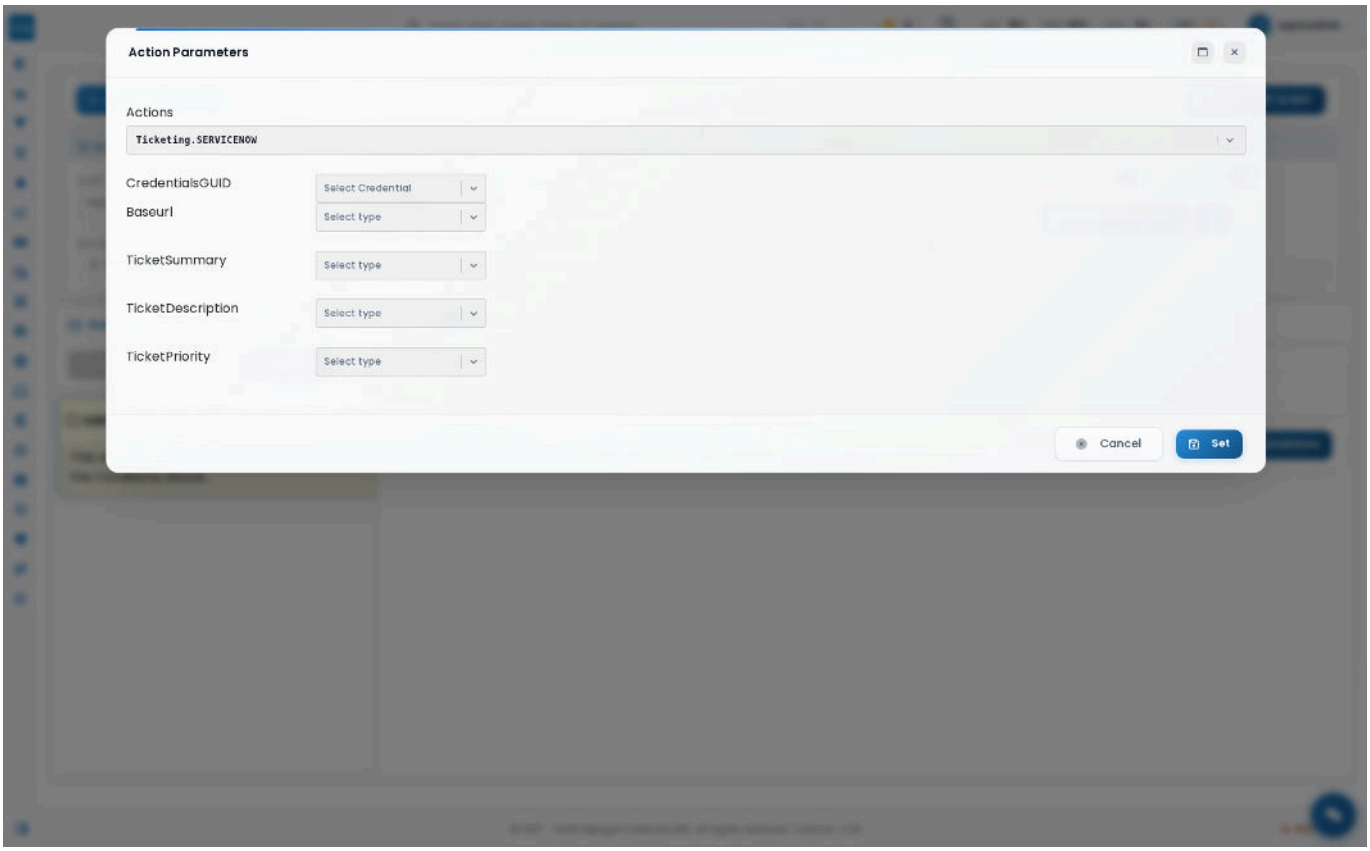
21.Ticketing.SERVICENOW / Ticketing.CONNECTWISE / Ticketing.REMEDY

These actions create a ticket directly in ServiceNow, ConnectWise Manage, or BMC Remedy/Helix ITSM when an alert is triggered. Each appears as its own entry in the action list.



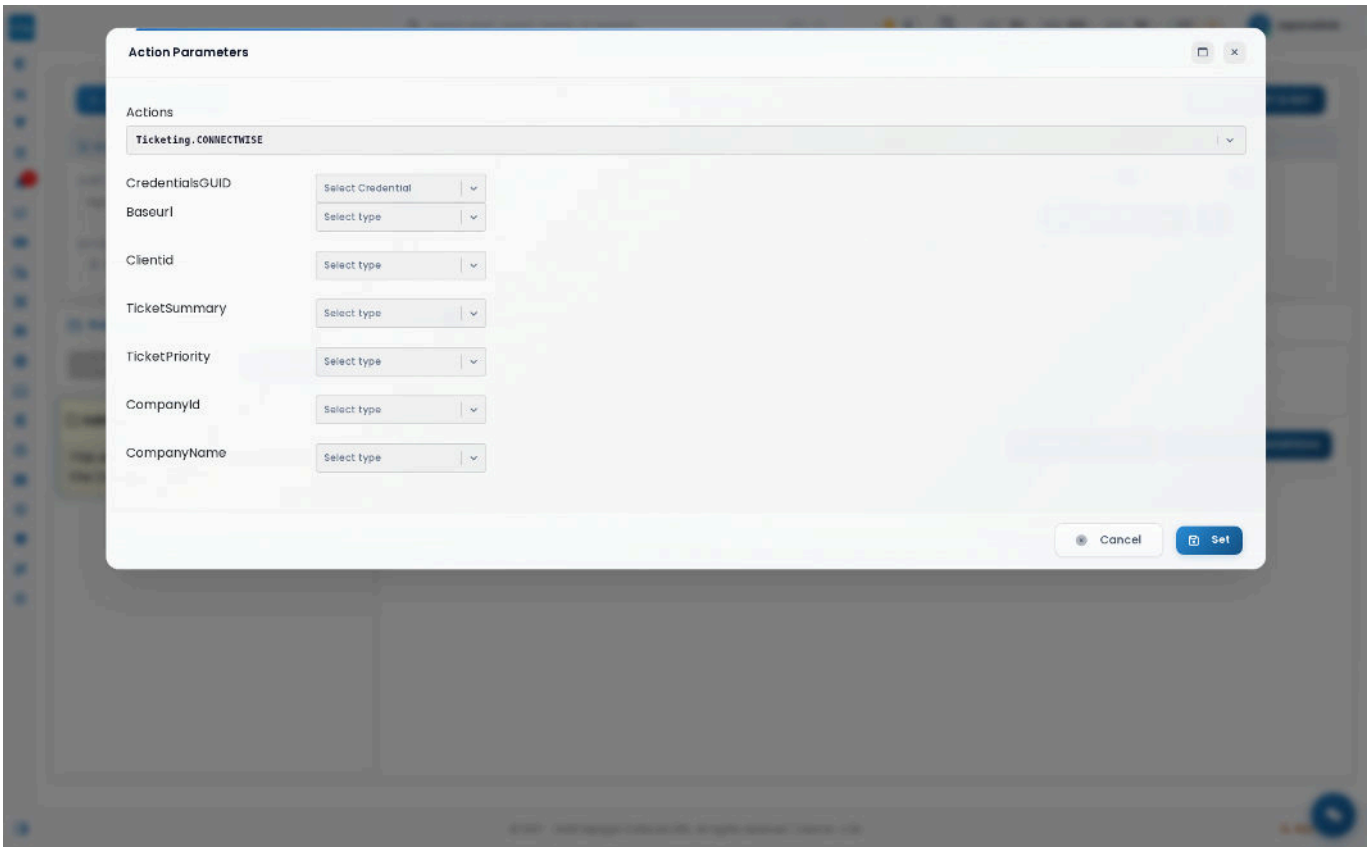
ServiceNow

- **CredentialsGUID** - The credential used to authenticate against the ServiceNow instance, selected from the credentials vault.
- **Baseurl** - The base URL of the ServiceNow instance.
- **TicketSummary** - The short description of the ticket to create.
- **TicketDescription** - The full description of the ticket to create.
- **TicketPriority** - The priority to assign to the ticket.



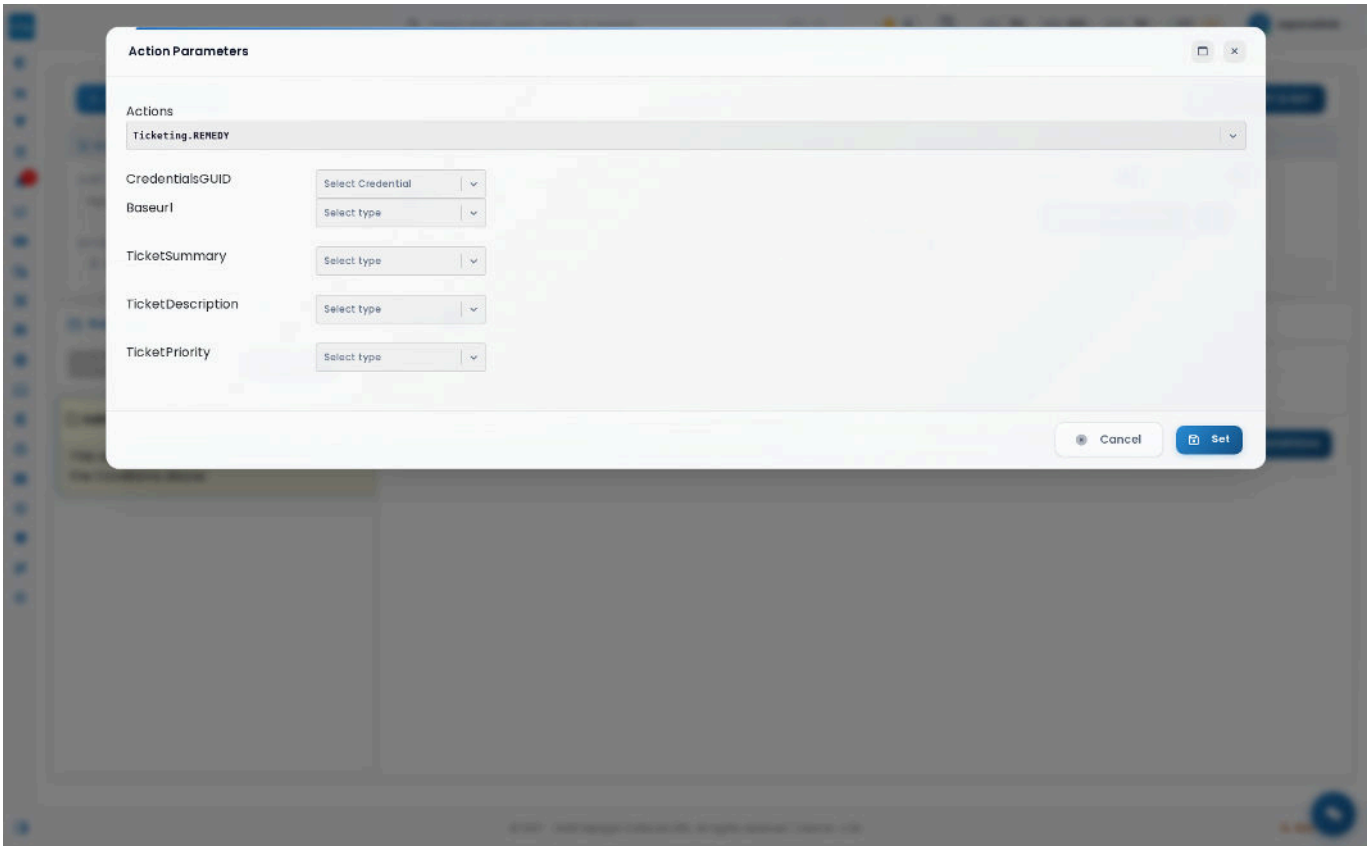
ConnectWise

- **CredentialsGUID** - The credential used to authenticate against ConnectWise Manage.
- **Baseurl** - The base URL of the ConnectWise instance.
- **Clientid** - The ConnectWise API client identifier.
- **TicketSummary** - The summary of the ticket to create.
- **TicketPriority** - The priority to assign to the ticket.
- **CompanyId** / **CompanyName** - The ConnectWise company the ticket is created under. Both are required.



Remedy

- **CredentialsGUID** - The credential used to authenticate against the Remedy/Helix ITSM instance.
- **Baseurl** - The base URL of the Remedy instance.
- **TicketSummary** - The short description of the incident to create.
- **TicketDescription** - The full description of the incident to create.
- **TicketPriority** - The priority to assign to the incident.



Operations · How to Add a New Asset

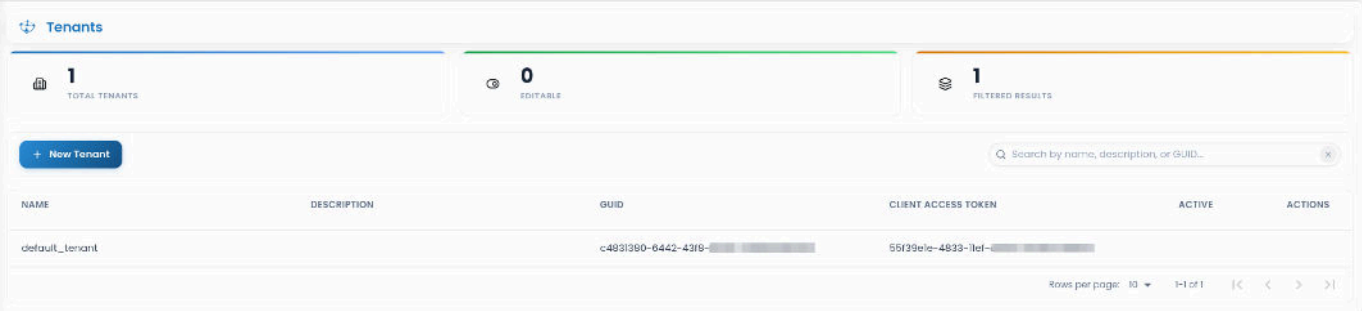
Overview

Assets in CYBERQUEST represent data source generators that automatically collect and process information from various sources. When data is collected, asset details are automatically populated by the system. Assets can be manually defined or existing asset details modified to ensure proper categorization and management.

Create Tenant

Tenants are used in CYBERQUEST instances that host multiple organizations or customers. To access tenant management, navigate to **Settings > Application Settings > Tenants**.

Note: *The default tenant is system-managed and cannot be modified.*



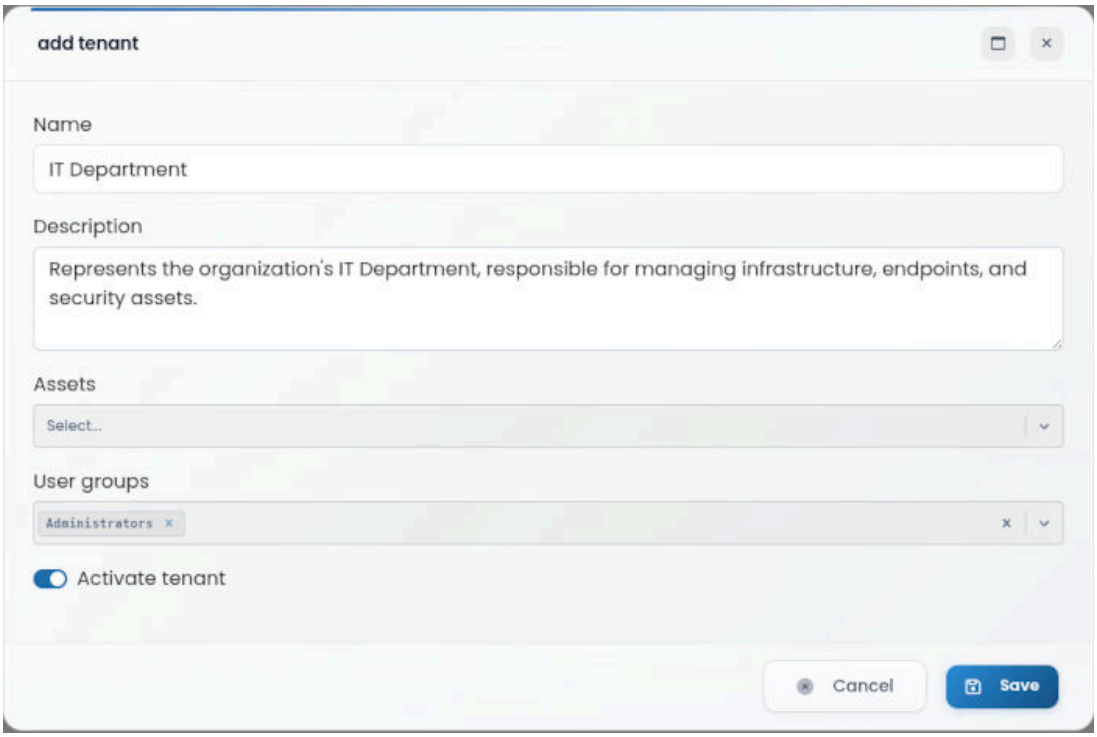
The Tenants page displays all configured tenants with the following options:

- **Edit** - Update or modify the details of an existing tenant.
- **Delete** - Remove a tenant from the system
- **NEW TENANT** - Add a new tenant to the instance.
- **Active/Inactive** - Enable or disable a tenant to control its active status.

To add a new tenant, click the



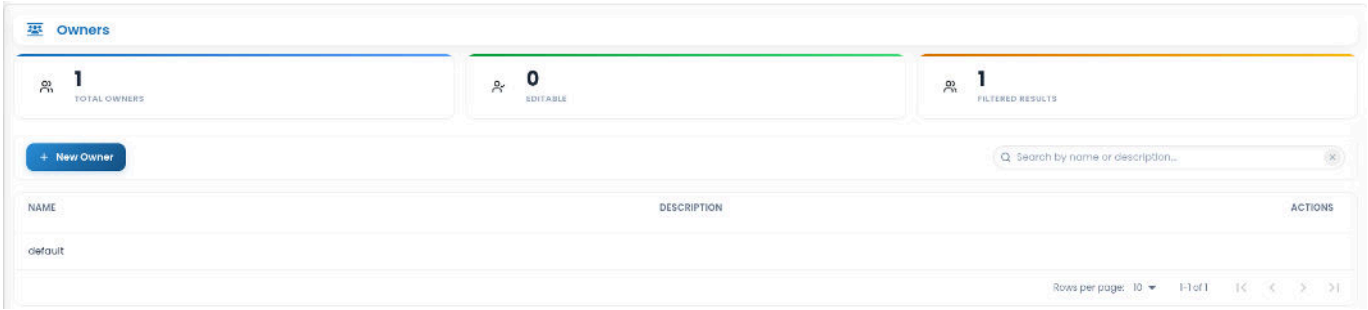
button, complete the tenant form with the required information, and then click **Save** to confirm or **Cancel** to discard the changes.



Create Owner

Owners represent the individuals or departments responsible for managing and overseeing assets. To access and manage owners, navigate to **Settings > Application Settings > Owners**.

Note: *The default owner is system-managed and cannot be modified.*



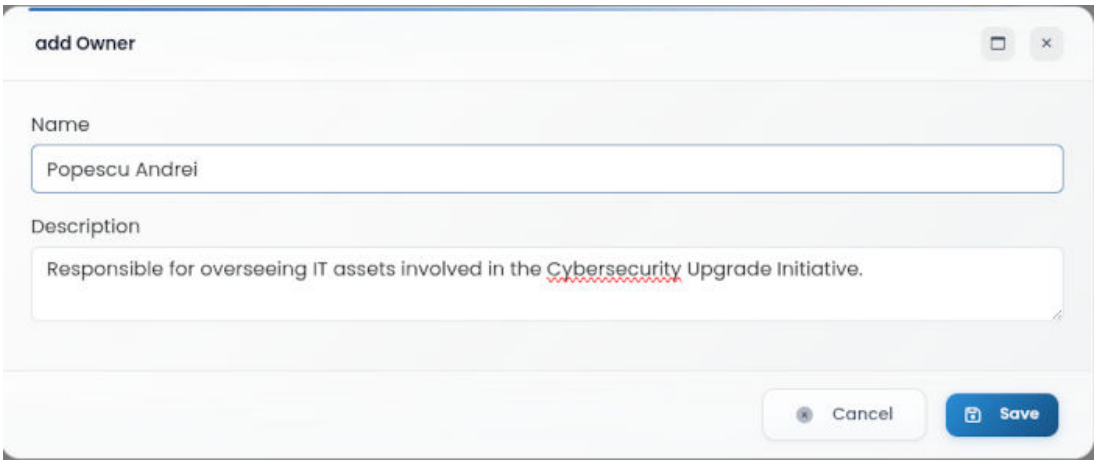
The Owners page shows all configured owners with management options:

- **NEW OWNER** - Create a new owner and assign ownership to assets.
- **Edit** - Update existing owner information.
- **Delete** - Remove an owner from the system when no longer required.

To add a new owner, click the **Add** button



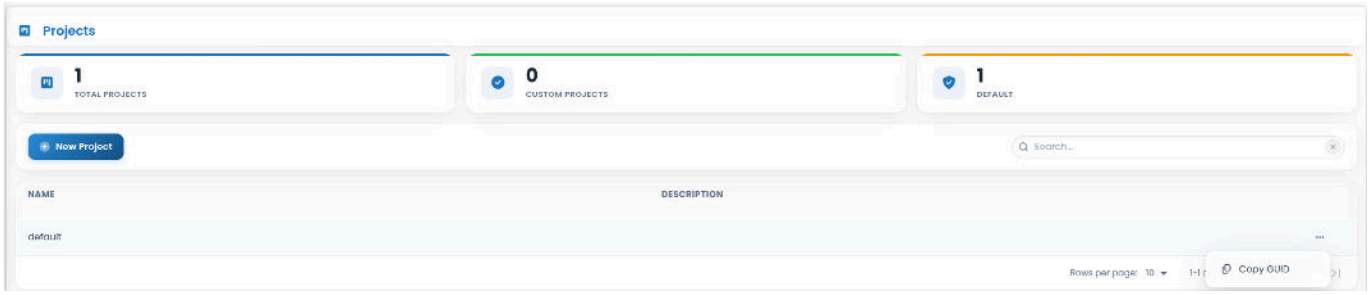
, complete the form with the owner's details (name, description), and click **Save** to confirm.



Create Project

Projects organize assets according to business initiatives, departments, or functional areas. To manage projects, navigate to **Settings > Application Settings > Projects**.

Note: *The default project is system-managed and cannot be modified.*



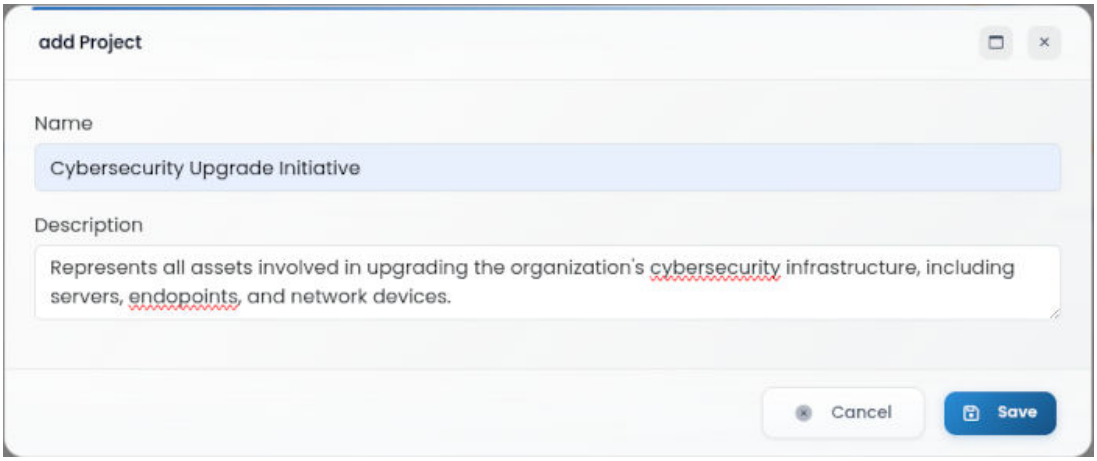
The **Projects** page lists all configured projects and provides options to manage them:

- **NEW PROJECT** - Create a new project and assign relevant assets.
- **Edit** - Update the details of an existing project.
- **Delete** - Remove a project from the system when it is no longer needed.

To add a new project, click the **Add** button



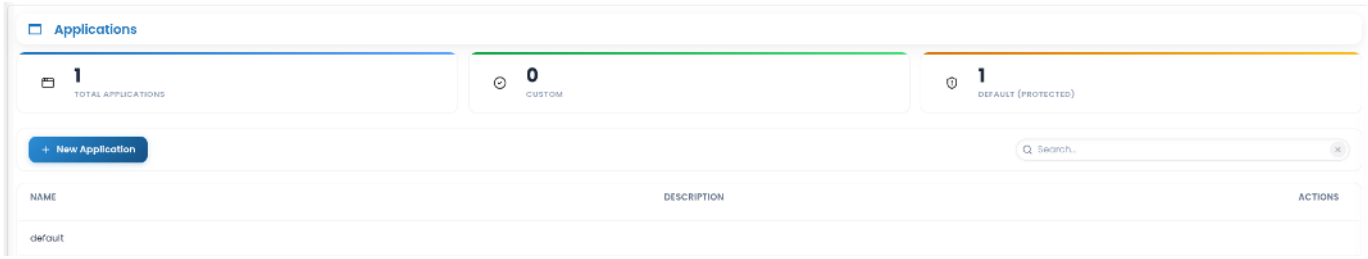
and complete the project form with the required details.



Create Application

Applications allow assets to be categorized by their function or software type. To manage applications, navigate to **Settings > Application Settings > Application**.

Note: *The default application is system-managed and cannot be modified.*



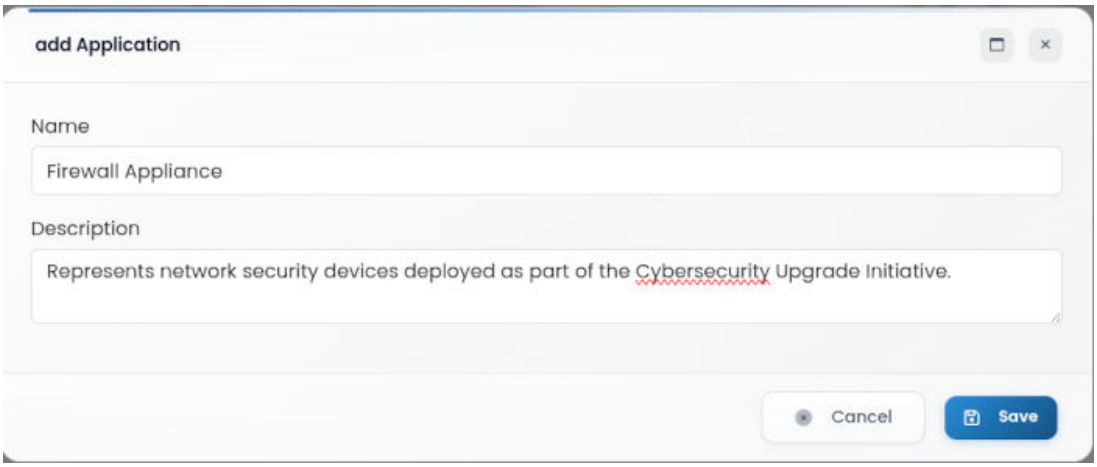
The **Applications** page lists all configured applications and provides options to manage them:

- **Add** - Create a new application category to organize assets.
- **Edit** - Update the details of an existing application.
- **Delete** - Remove an application from the system when it is no longer needed.

To add a new application, click the **Add** button



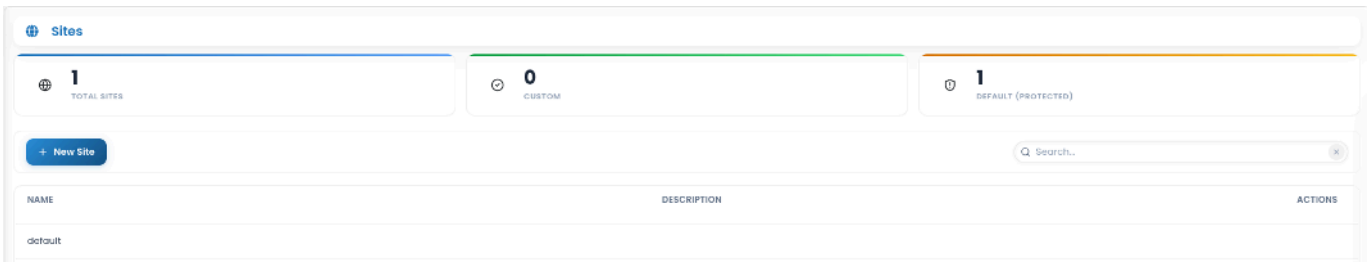
and complete the form with the application details.



Create Site

Sites represent physical locations, data centers, or logical environments where assets are deployed. To manage sites, navigate to **Settings > Application Settings > Sites**.

Note: *The default site is system-managed and cannot be modified.*



The **Sites** page lists all configured sites and provides options to manage them:

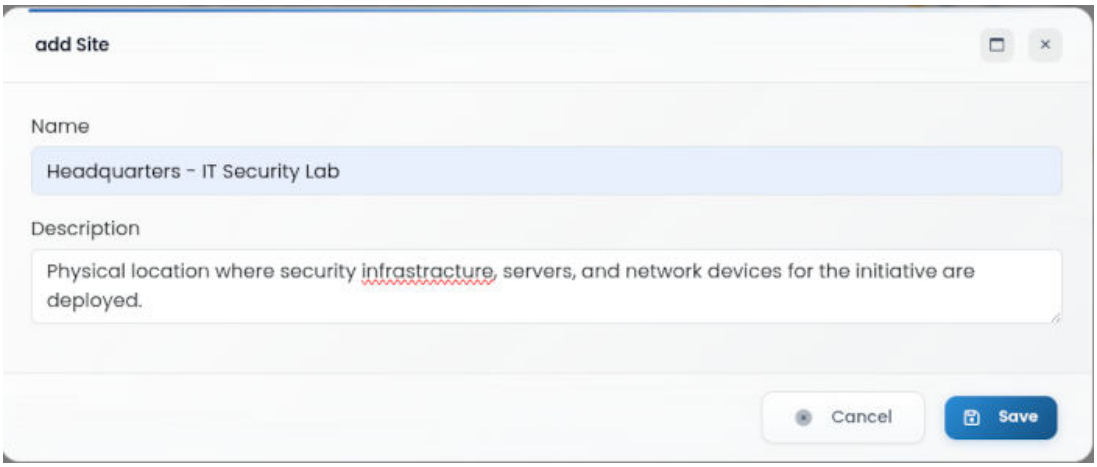
- **Add** - Create a new site to organize assets by location or environment.
- **Edit** - Update details for an existing site.

- **Delete** - Remove a site from the system when it is no longer needed.

To add a new site, click the **Add** button



and complete the form with the site details.



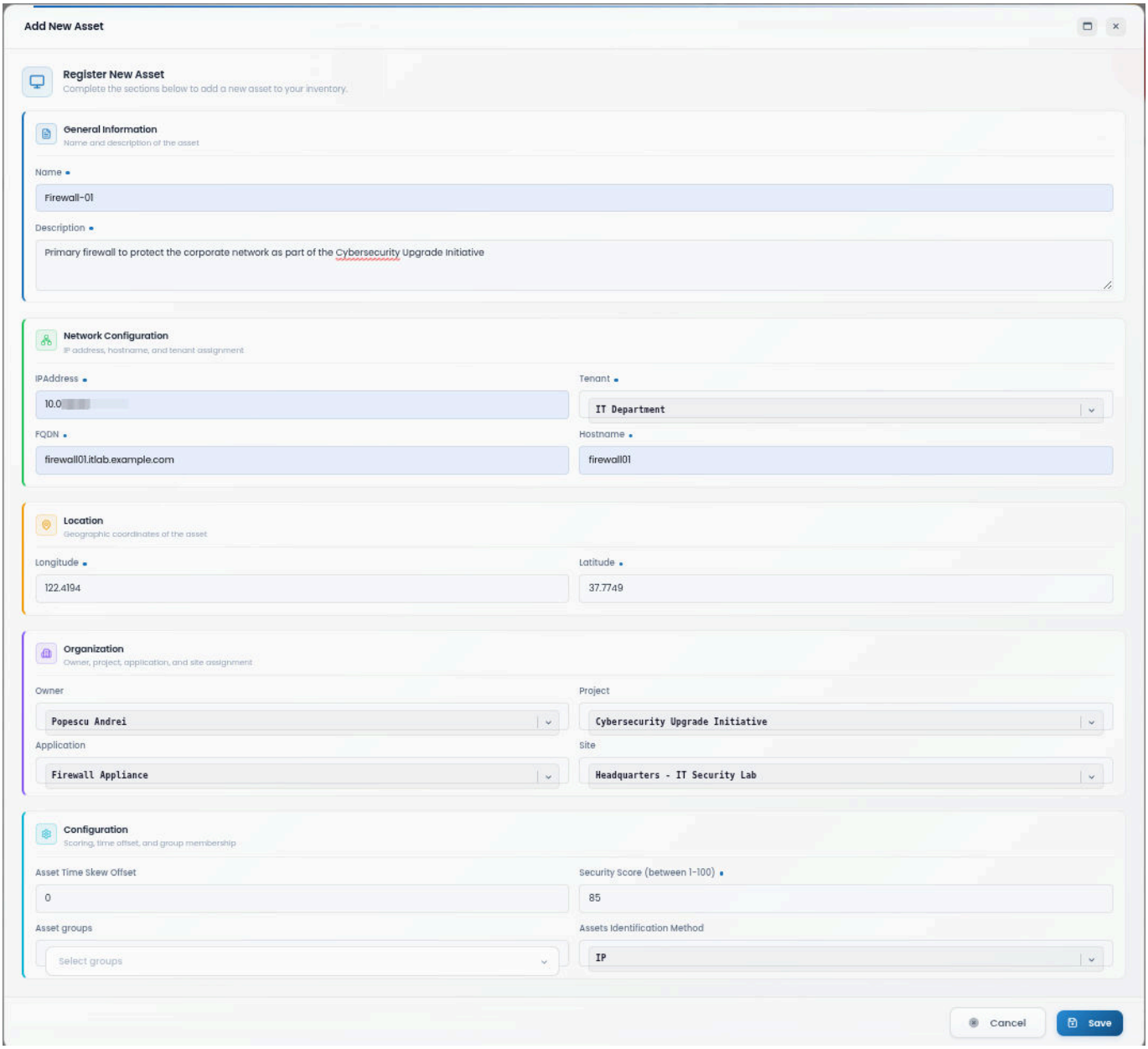
Add New Asset

Once all prerequisites are configured, assets can be added to the system. To manage assets, navigate to **Settings > Application Settings > Assets**.

To add a new asset, click the **Add** button



to open the asset configuration window.



The asset configuration form includes the following fields:

- **Name** - The asset identifier. Can be automatically assigned by CYBERQUEST during data collection or manually defined by the user
- **Description** - Detailed information about the asset's purpose and function
- **FQDN** - Fully Qualified Domain Name (e.g., server.example.com) - the complete domain name for a specific computer or host
- **Hostname** - The short domain name assigned to a host computer (e.g., server)
- **Longitude** - Geographic longitude coordinate of the asset's location
- **Latitude** - Geographic latitude coordinate of the asset's location
- **Tenant** - Assign the asset to a specific tenant (for multi-tenant deployments)
- **Owner** - Select the owner responsible for this asset
- **Project** - Choose the project associated with this asset
- **Application** - Select the application category for this asset

- **Site** - Specify the site where this asset is located
- **Asset Time Skew Offset** - Time difference in seconds between the asset's clock and the CYBERQUEST server clock. Important for accurate timestamp correlation
- **Security Score (1-100)** - A numerical representation of the asset's security posture
- **Asset Groups** - Groups that the asset belongs to, used for bulk operations and policy management
- **Assets Identification Method** - How the asset will be identified: IP address, FQDN, or Hostname

Assets can be created using default values for **Owner**, **Project**, **Application**, and **Site**, or customized according to the configuration steps outlined in the prerequisites.

Assets assigned to the **DEFAULT** category are those that cannot be accurately categorized at the time of creation. This typically includes:

- Assets with incomplete configuration details
- Newly discovered assets awaiting proper classification
- Assets that do not match any existing organizational structures

Operations · How to avoid split brain in MariaDB galera replication

CYBERQUEST MariaDB Galera Replication

Split-brain in a database cluster like Galera Cluster for MySQL refers to a situation where two or more nodes in a cluster start to accept writes independently of each other, leading to data inconsistencies. Preventing split-brain scenarios is crucial for the integrity and reliability of CYBERQUEST's database in a multi-master scenario.

Recommendations to avoid split-brain in a CYBERQUEST MariaDB Galera DB cluster:

1. Use a Minimum of Three Nodes: Having at least three nodes can help in reaching quorum, which is important for deciding the primary component during network partitions. With two nodes, it's easy for both to think they are primary in case of a partition. Use at least 1 "witness" read-only node.
2. Use the 'pc.weight' Parameter: This parameter can be used to give more voting power to specific nodes. If you know a particular node has more reliable network connectivity or is more trusted, you can give it more weight in the cluster decisions.
3. Enable wsrep_auto_increment_control: By default, this is enabled. It helps in avoiding simultaneous auto-increment collisions when there are simultaneous writes on multiple nodes.
4. Use gcache.size: This parameter ensures there is a retained write-set cache. It's beneficial when nodes that went out of sync want to rejoin without doing a full state snapshot transfer.
5. Avoid Using Asynchronous Replication in Parallel
6. Watch the Network: Unreliable network connections are a common cause for split-brain. Regularly check and maintain the physical and virtual network components.
7. Assign dedicated replication network interfaces to the nodes to ensure proper communication
8. Use Galera Arbitrator (GARBD): If you are running an even number of nodes, consider using Galera Arbitrator. It's a lightweight process that can act as an additional vote during network partitions but doesn't store data.

   Tune Failure Detection Parameters: evs.inactive_timeout adjusts the time it takes to declare a node inactive. evs.suspect_timeout adjusts the time after which a non-responding node is suspected to be down.

Proper tuning can help in avoiding premature node evictions.

Monitor the Cluster: Use monitoring tools to regularly check the health and status of nodes, ensuring they are in sync. Address any node outages or network interruptions quickly.

Test Scenarios: Regularly simulate network partitions, node failures, and other disruptions in a staging environment to understand how your cluster reacts and to fine-tune settings.

9. Educate Your Team: Ensure your team understands the importance of not writing to multiple nodes when the cluster is partitioned.

0. Documentation and Procedures: Have clear documentation about what to do in the event of a network partition or node failure, and regularly review and update these procedures.

Finally, while MariaDB Galera Cluster offers synchronous replication which inherently reduces the risk of split-brain compared to asynchronous replication methods, it's always important to understand the configuration and operational aspects of any technology to ensure it behaves as expected in various scenarios.

Operations · How to Change CYBERQUEST Administrative Passwords

CYBERQUEST has default users with administrative rights:

- Virtual or physical appliance users (Linux):
  - superadmin
  - root
- Web application users:
  - superadmin

This guide explains how to change passwords for the appliance *superadmin* and *root* users (the administrative users for the machine that hosts the CYBERQUEST processing server - usually a VM running Debian or Ubuntu).

Note: For web application passwords, see: How to change web application superadmin password.

On the virtual machine (VM), the *superadmin* account can connect via SSH or console and has sudo privileges on the machine.

The *root* account should be reserved for critical system operations only. Prefer `sudo` via the *superadmin* account; root may be disabled by policy.

To change passwords for the appliance administrative users (*superadmin* and *root*) use the following procedure:

Access CYBERQUEST server

Access the CYBERQUEST server via SSH or console and log in with the *superadmin* user.

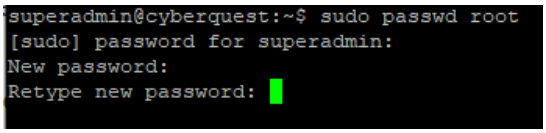
Example SSH command:

```
ssh superadmin@CYBERQUEST_IP_OR_HOSTNAME
# If using a custom port:
ssh -p 2222 superadmin@CYBERQUEST_IP_OR_HOSTNAME
```

Changing root & superadmin password

To change the *root* account password, run:

```
sudo passwd root
```

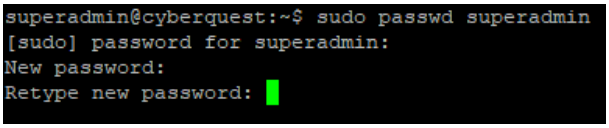


To change the *superadmin* account password while logged in as that user, run:

```
passwd
```

Alternatively:

```
sudo passwd superadmin
```



Verify changes

1.Reconnect via SSH using the new superadmin password:

```
ssh superadmin@CYBERQUEST_IP_OR_HOSTNAME
```

2.Force a sudo prompt and verify the new password:

```
sudo -k
sudo -l
```

3.If the root password has been changed, verify the update:

```
su - root
```

Operations · How to change password web application superadmin password

How to Change CYBERQUEST Web Application Passwords

A user can change their own password from the User menu. This is strongly recommended after the first login and can be performed at any time. Also, a user with administrative rights can change the passwords of other users.

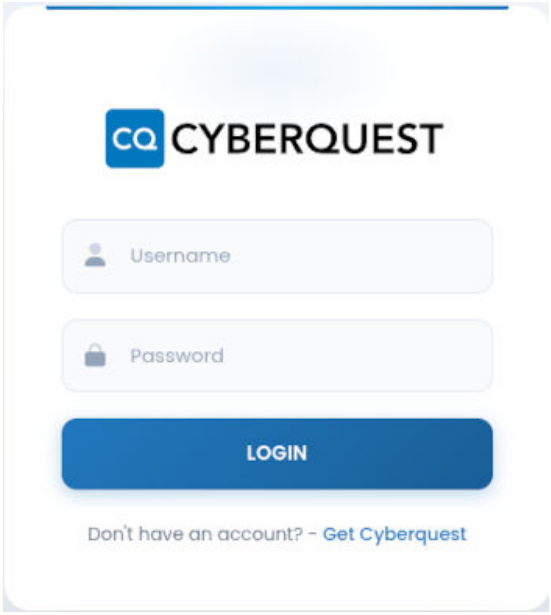
To change the password, follow these steps:

Change own password

Step 1. Authentication

To access Web Interface, open a web browser and type the application's address or DNS name. The default address initially assigned to Web Interface is ***https://CyberquestIPAddress*** (example).

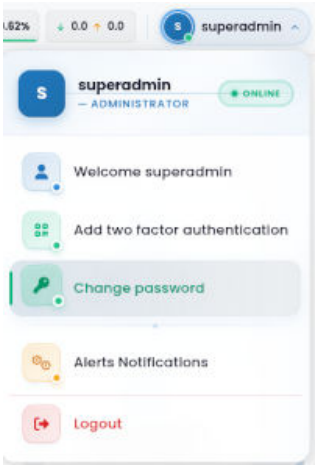
The browser automatically redirects you to CYBERQUEST's authentication page:



Note: If the organization uses SSO/LDAP/SAML, password changes may be managed by the identity provider and this option can be disabled. Use the IdP self-service portal in that case.

Step 2. Navigate to User actions

To change the password, go to **User menu (top-right) > Change password**.



Step 3. Complete the form with passwords

Complete the form:



- In the **Old Password** field, enter the current password.

- In the **New Password** field, enter the new password, ensuring it meets the complexity requirements for the environment.
- Re-enter the new password in the **Confirm Password** field.

Press "**Save**" to save the new password and close the window, or press "**Cancel**" to close the window without saving changes.

Verification

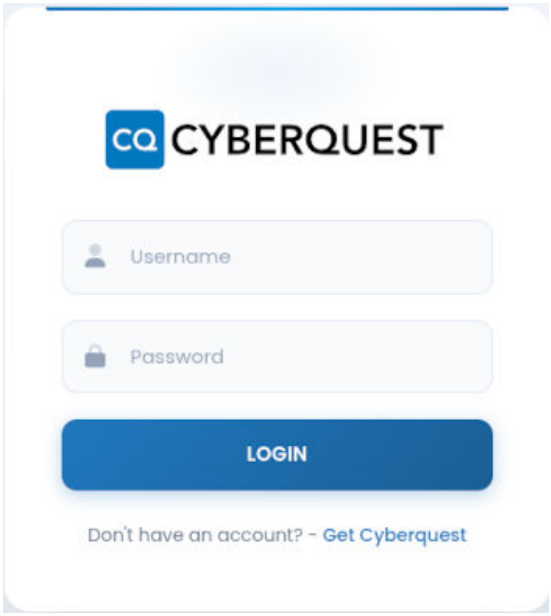
Log out and log back in using the new password to confirm the change.

Change another user's password

Step 1. Authentication

To access Web Interface, open a web browser and type the application's address or DNS name. The default address initially assigned to Web Interface is ***https://CyberquestIPAddress*** (example).

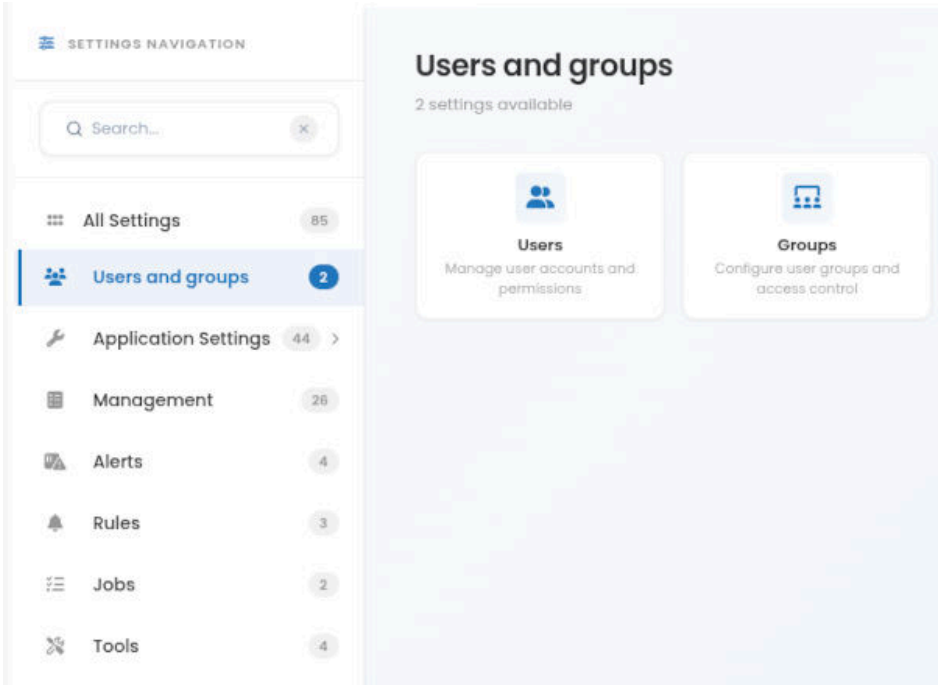
The browser automatically redirects you to CYBERQUEST's authentication page:



Step 2. Changing Password

An administrator with user management privileges can update their own password as well as the passwords of other users by following these steps:

a. In **Settings** menu, click **Users and Groups > Users**:



Users configuration page opens:



b. Click



for the target user. Complete the form:



- In the **New Password** field, enter the new password, ensuring it meets the environment's complexity requirements.
- Re-enter the new password in the **Confirm Password** field.

Press "**Save**" to save the new password and close the window, or press "**Cancel**" to exit without saving. Alternatively, the window can be closed without saving by clicking the



in the top-right corner.

After resetting another user's password, ensure the user logs in with the new password and updates it if required by policy.

Operations · How to collect data from Check Point Firewall

This document explains how to add a new data source - **Check Point Firewall** - using syslog forwarding.

Before adding the data source in CYBERQUEST, configure the Check Point Firewall to forward events to the CYBERQUEST server on **UDP port 5140**.

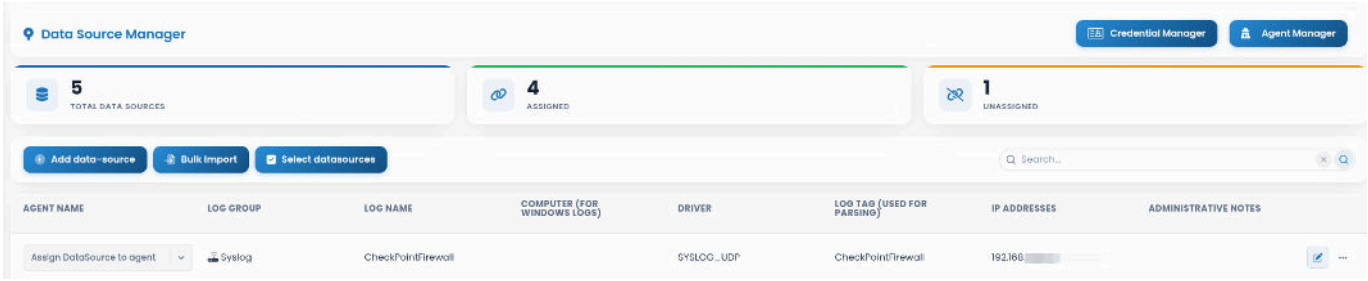
For detailed setup instructions, refer to the configuration guide: Configure Check Point Firewall Log Forwarding to CQ

Navigate to Settings

Log in to the **CYBERQUEST** web interface with an account that has **administrator privileges**.

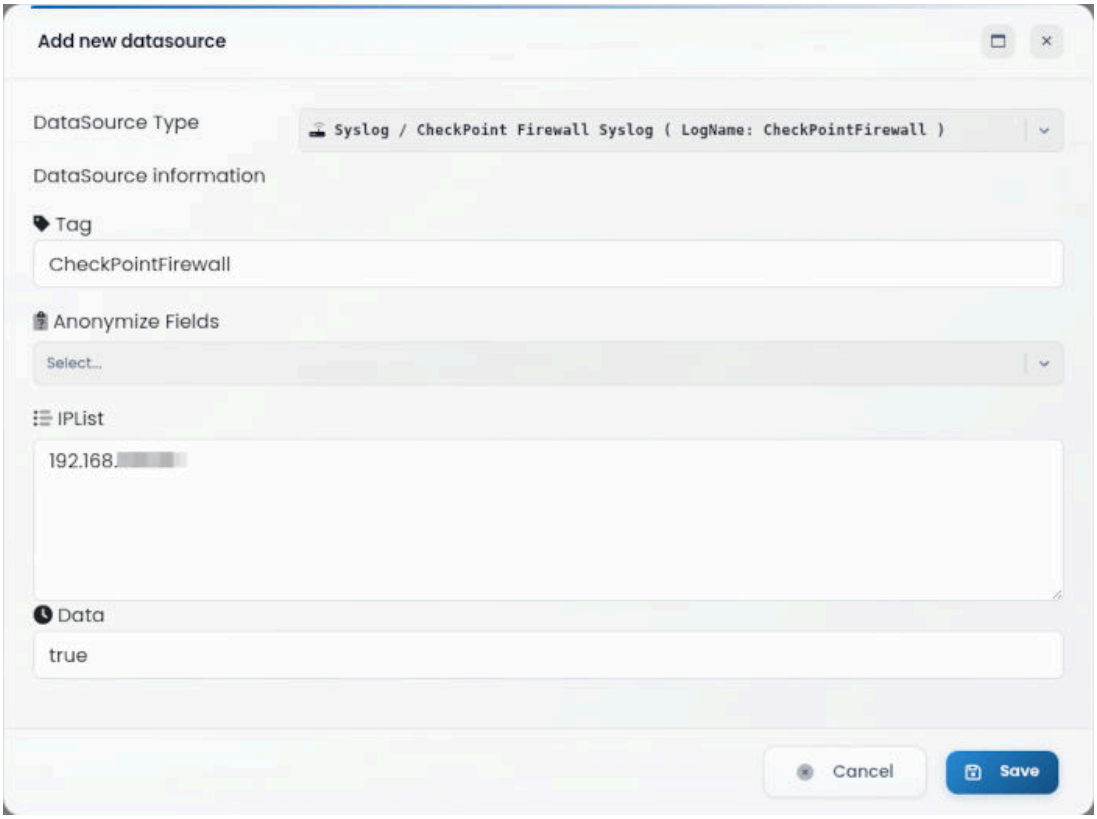
Navigate to **Settings** > **Management** > **Data Source Manager**.

This page contains all the data sources added in the CYBERQUEST application.



Add data source

Press the **ADD DATA-SOURCE** button and complete the following form:



- **DataSource Type:** Choose **"Syslog / CheckPoint Firewall Syslog (LogName: CheckPointFirewall)"** to interpret Check Point Firewall events.

- **DataSource Information:** This field is populated automatically with the data source details.
- **Tag:** A unique identifier automatically assigned to the data source;
- **Anonymize Fields:** Select one or more fields to be anonymized as required.
- **IPList:** Enter the sender IP address(es) for this source, separated by commas. CYBERQUEST will accept logs only from these IPs.
- **Data:** `true` = active and receiving logs; `false` = inactive or not receiving logs.

Click the "Save" button to save the data source.

Verify ingestion

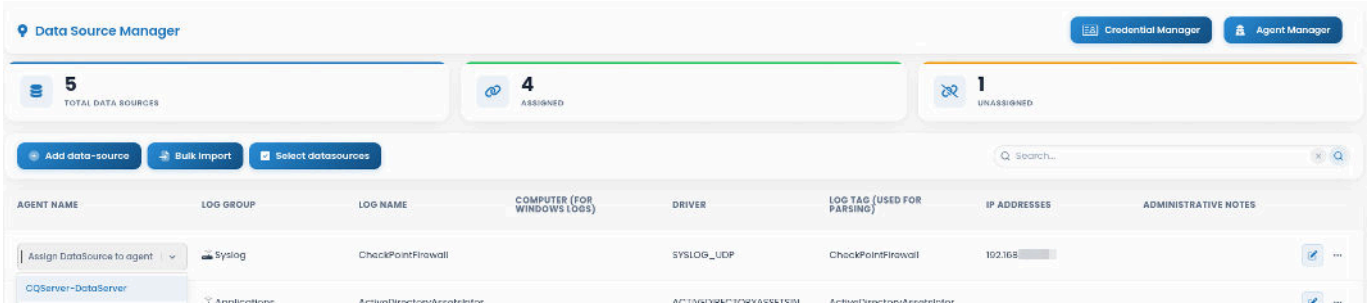
- On the CQ server, confirm packets are received:

```
sudo tcpdump -n udp port 5140 -i any
```

- In CYBERQUEST, open the **Browser** to verify that Check Point events are appearing and tagged as `CheckPointFirewall`.

Assign the CYBERQUEST agent

The next step is to assign the CYBERQUEST agent to this data source. Press the drop-down list and choose the agent (often the CQServer-DataServer agent):



- **Edit**: Press

  to modify the data source information. The process is very similar to adding a new data source.

- **Clone:** Press

  button to create a copy of the data source.

- **Delete:** To remove a data source, unassign the Agent first, then press **"Delete"**.

Operations · How to collect data from the Office 365 application

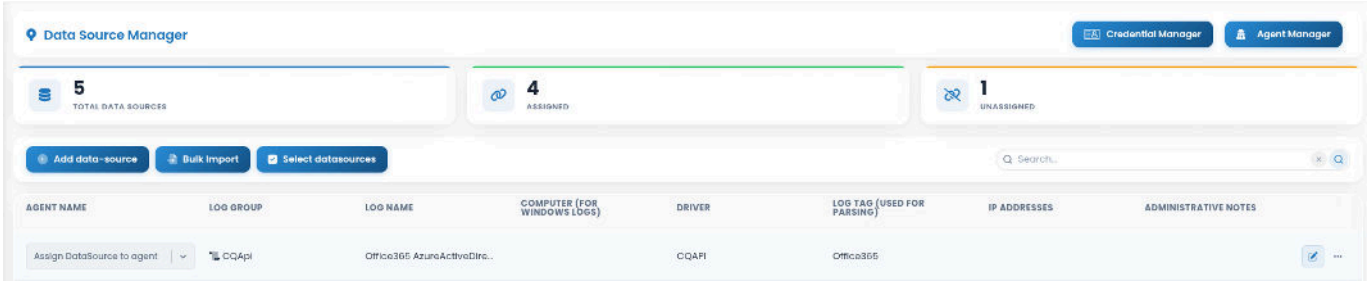
This page describes how to collect events from the Office 365 data source.

Navigate to Settings

Log in to the **CYBERQUEST** web interface with an account that has **administrator privileges**.

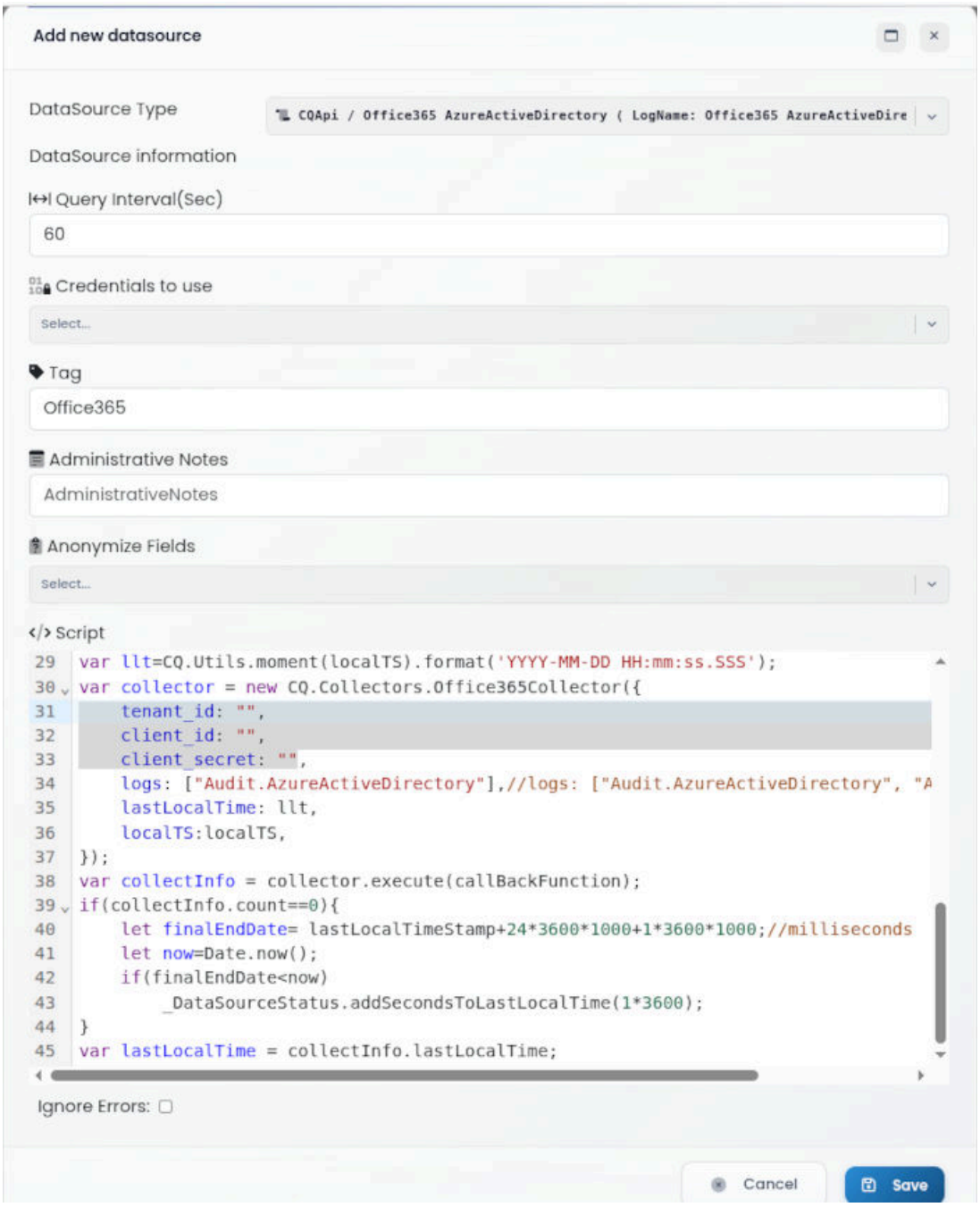
Navigate to **Settings** > **Management** > **Data Source Manager**.

This page contains all the data sources added in the CYBERQUEST application.



Complete the form

Press the "ADD DATA-SOURCE" button and complete the following form:



- **DataSource Type:** Select one of the three Office 365 data sources: "CQApi / Office365 AzureActiveDirectory (LogName: Office365 AzureActiveDirectory)", "CQApi / Office365 Exchange (LogName: Office365 Exchange)", or "CQApi / Office365 Sharepoint (LogName: Office365 Sharepoint)";
- **Query Interval:** How often the query runs. Defaults to every 60 seconds;

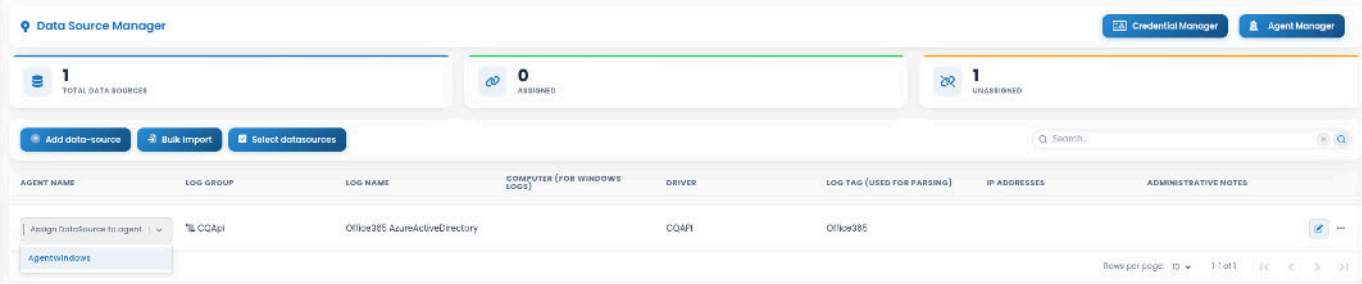
- **Credentials to use:** Select appropriate credentials from the drop-down list (See Credential Setup: How to manage Credentials;
- **Tag:** A unique identifier automatically assigned to the data source;
- **Administrative Notes:** Optional notes for administrators;
- **Anonymize Fields:** Select fields to be anonymized. One or more options can be selected;
- **Script:** Complete the following keys in the script:

```
tenant_id: "Directory (tenant) ID"
client_id: "Application (client) ID"
client_secret: "Client Secrets / secret key"
```

Click the “Save” button to save the data source.

Assign the CYBERQUEST agent

The next step is to assign the CYBERQUEST agent to this data source. Press the drop-down list and choose the agent (often the CQ Server agent).



- **Edit:** Press

  button to modify the data source information. The steps are very similar to adding a new data source.

- **Clone:** Press the

  to create a copy of the data source.

- **Delete:** To remove a data source, first unassign the Agent, then press **“Delete”**.

Operations · How to collect data on Active Directory Assets Information

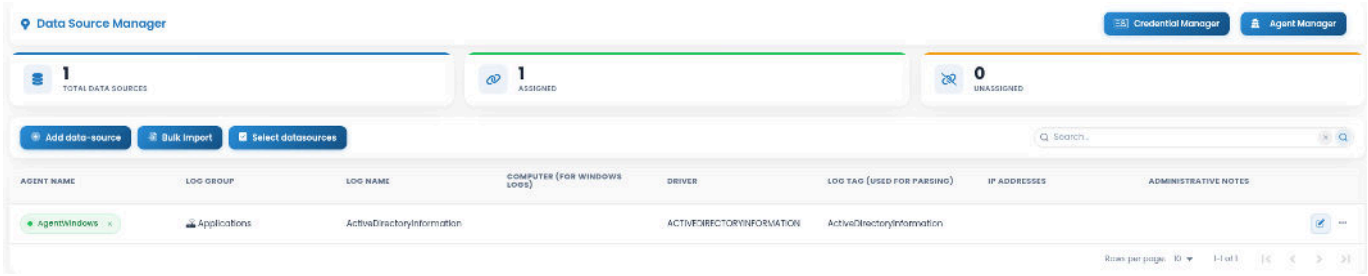
This page describes how to collect events from the ActiveDirectoryAssetsInformation data source.

Navigate to Settings

Log in to the CYBERQUEST web interface with an account with administrative rights.

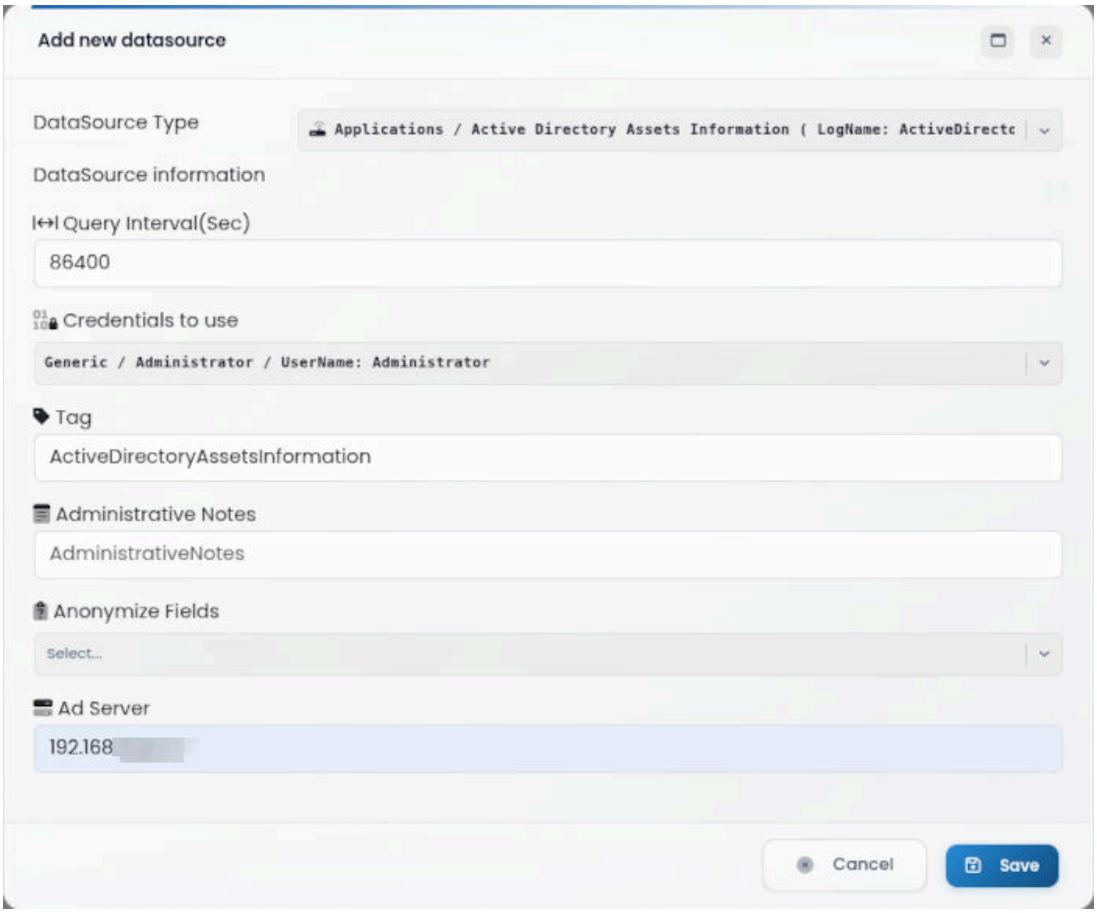
Navigate to **Settings** > **Management** > **Data Source Manager**.

This page contains all the data sources added in the CYBERQUEST application.



Complete the form

Press the “Add data-source” button and complete the following form:



DataSource Type: Select “Applications/Active Directory Assets Information (LogName: ActiveDirectoryAssetsInformation)” data source type;

DataSource Information: This field is filled in automatically with data source information;

Query Interval: How often the query runs. Defaults to every 86400 seconds;

Credentials to use: Select a domain account with read access to Active Directory from the drop-down list (See Credential Setup: How to manage Credentials);

Tag: A unique identifier automatically assigned to the data source;

Administrative Notes: Optional notes for administrators;

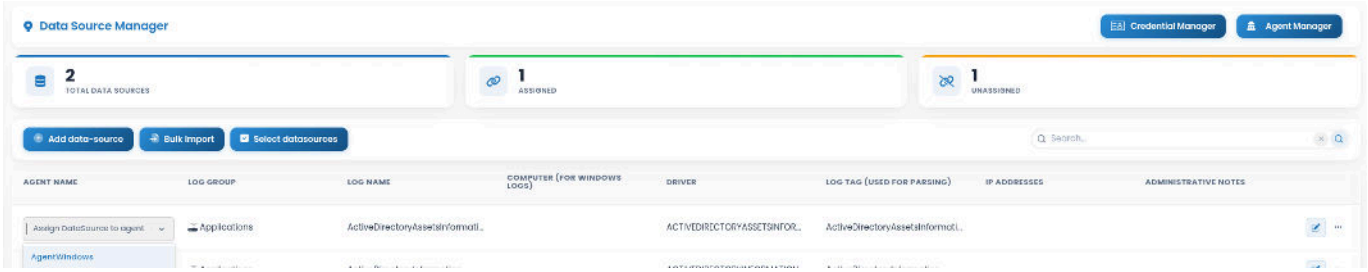
Anonymize Fields: Select fields to be anonymized. One or more options can be selected;

AD Server: Enter the FQDN or IP of the Active Directory server;

Click the “Save” button to save the data source.

Assign the CYBERQUEST agent

The next step is to assign the CYBERQUEST agent to this data source. Use the drop-down list to choose the agent.

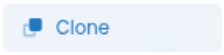


- **Edit:** Click the

  button to update the data source information. The steps are similar to adding a new data source.

- **Clone:** Click the

  to create a duplicate of the data source.

- **Delete:** To remove a data source, unassign the Agent first, then click **"Delete"**.

Operations · How to collect data on Active Directory

This page describes how to collect events from the Windows Active Directory data source.

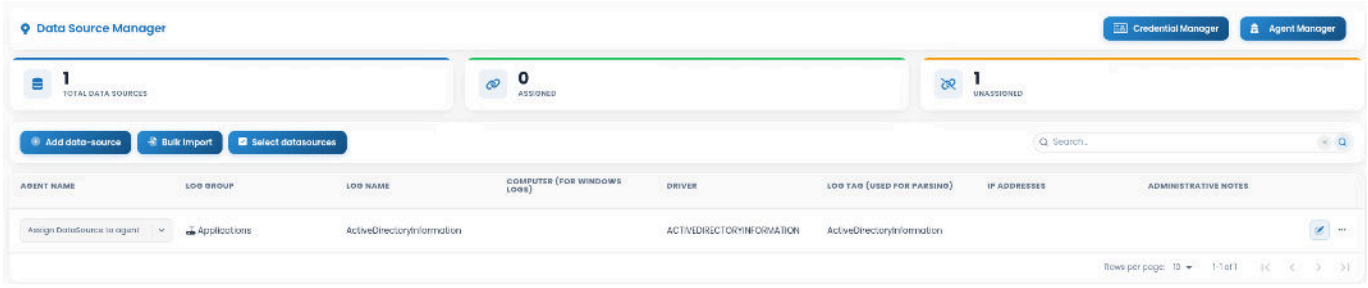
Navigate to Settings

Log in to the CYBERQUEST web interface with an account with administrative rights.

Navigate to **Settings > Management > Data Source Manager**.

Data Source Manager

This page contains all the data sources added in the CYBERQUEST application.

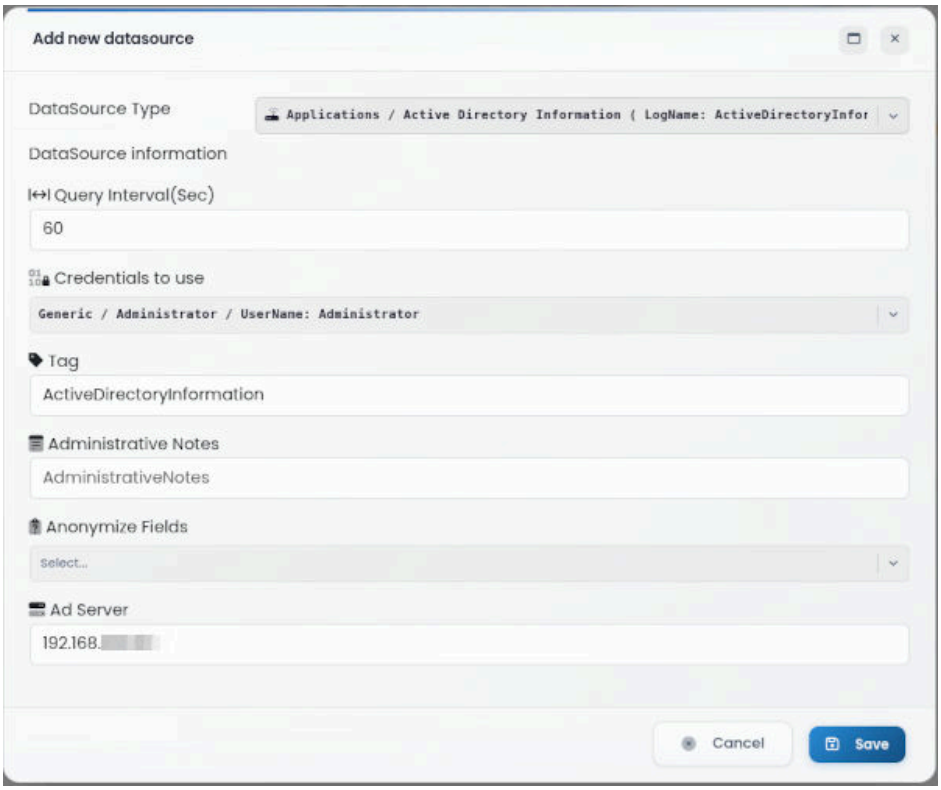


Add data source

To add a new data source, press



and complete the following form:

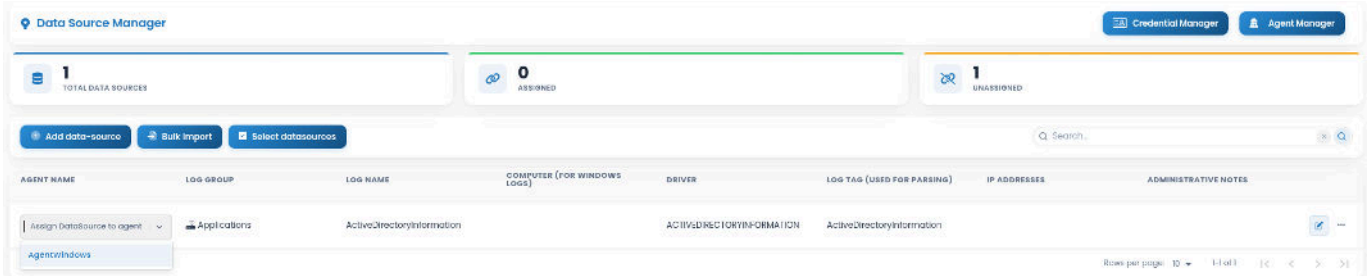


- **DataSource Type:** Select "Applications / Active Directory Information (LogName: ActiveDirectoryInformation)" data source type;
- **DataSource Information:** This field is filled in automatically with data source information;
- **Query Interval:** How often the WMI (Windows Management Instrumentation) query runs. Defaults to every 60 seconds;
- **Credentials to use:** Select a domain account with WMI and directory read permissions (See Credential Setup: How to manage Credentials);
- **Tag:** A unique identifier automatically assigned to the data source;
- **Administrative Notes:** Optional notes for administrators;
- **Anonymize Fields:** Select fields to be anonymized. One or more options can be selected;
- **Computer:** Enter the FQDN or IP of the target Domain Controller or server;

Complete the form and press "**Save**" to save changes, or "**Cancel**" to close the window without saving.

Assign the CYBERQUEST agent

The next step is to assign the CYBERQUEST agent to this data source. Press the drop-down list and choose the agent.



- **Edit:** Click the

  button to update the data source information. The steps are similar to adding a new data source.

- **Clone:** Click the



to create a duplicate of the data source.
- **Delete:** To remove a data source, unassign the Agent first, then click **“Delete”**.

Operations · How to collect data on Windows Application Log

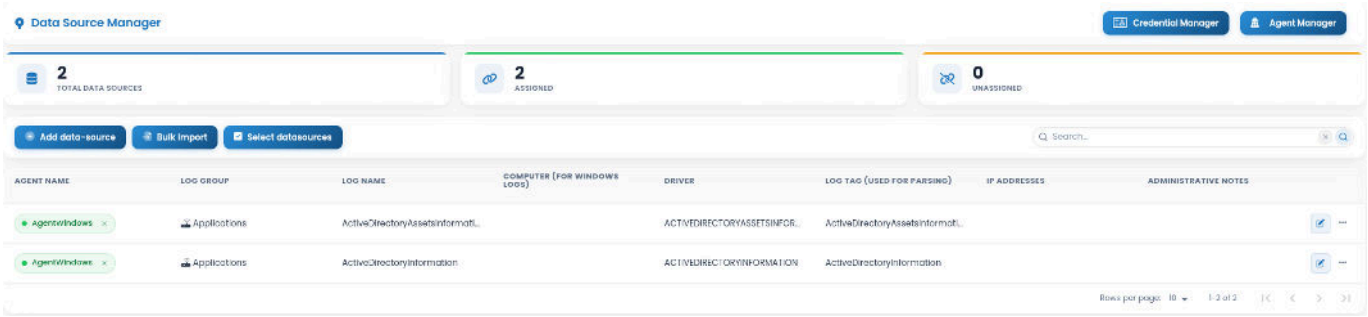
This page describes how to collect events from the Windows Application data source.

Navigate to Settings

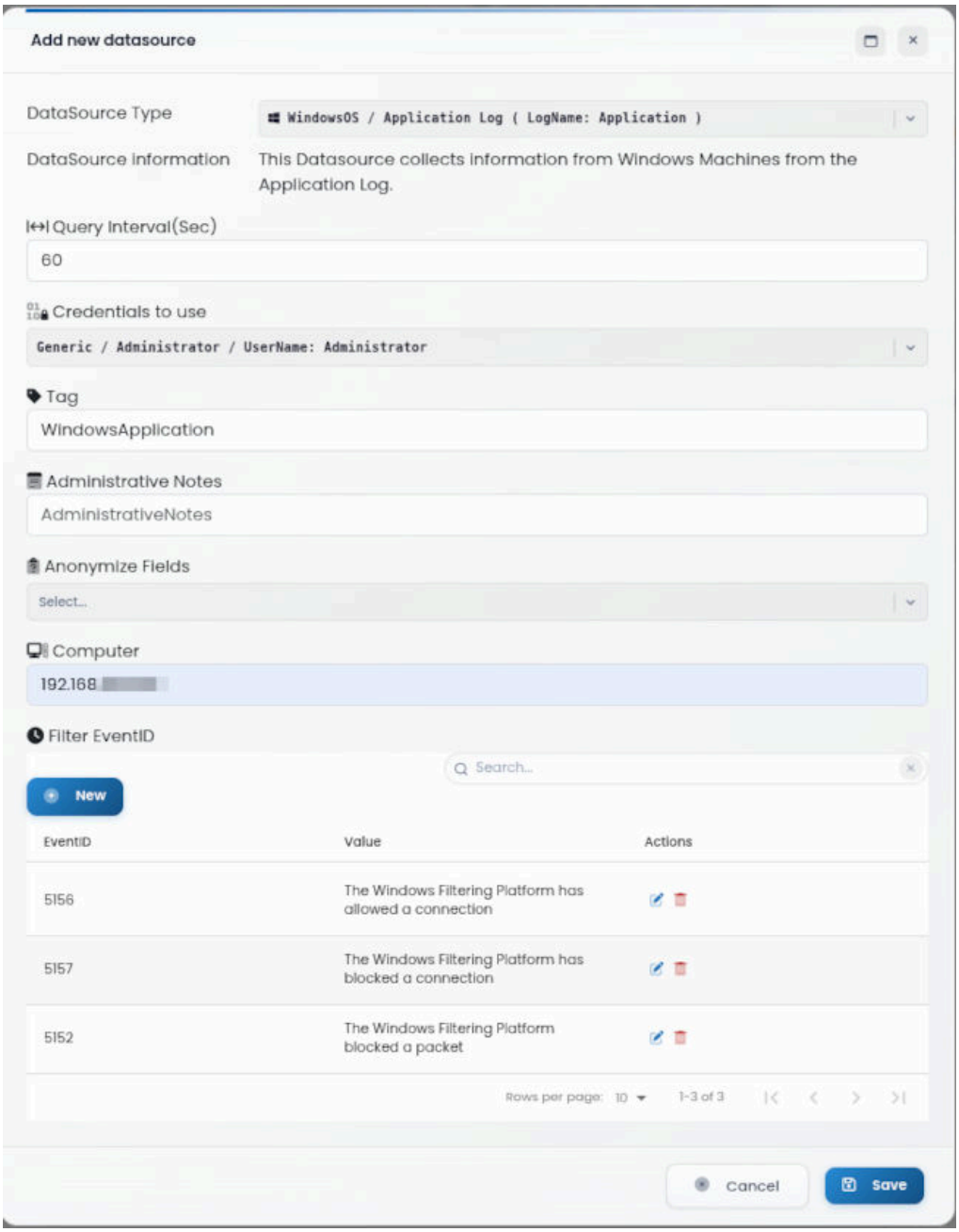
Log in to the CYBERQUEST web interface with an account with administrative rights.

Navigate to “**Settings** > **Management** > **Data Source Manager**”.

This page contains all the data sources added in the CYBERQUEST application.



Press the “Add data-source” button and complete the following form:



- **DataSource Type:** Select "WindowsOS/ Application Log (LogName: Application)" data source type;
- **DataSource Information:** This field is filled in automatically with data source information;
- **Query Interval:** How often the WMI (Windows Management Instrumentation) query runs. Defaults to every 60 seconds;
- **Credentials to use:** Select a domain or local account with permissions to read Windows Event Logs and WMI (See Credential Setup: How to manage Credentials);
- **Tag:** A unique identifier automatically assigned to the data source;
- **Administrative Notes:** Optional notes for administrators;
- **Anonymize Fields:** Select fields to be anonymized. One or more options can be selected;
- **Computer:** Enter the hostname (FQDN) or IP address of the Windows host;

Click the "Save" button to save the data source.

Assign the CYBERQUEST agent

The next step is to assign the CYBERQUEST agent to this data source. Press the drop-down list and choose the agent.



Actions menu

- **Edit:** Click the

  button to update the data source information. The steps are similar to adding a new data source.

- **Clone:** Click the

  to create a duplicate of the data source.

- **Delete:** To remove a data source, unassign the Agent first, then click **“Delete”**.

To delete a data source, unassign the Agent first, then press “Delete”.

Operations · How to collect data on Windows Security Log

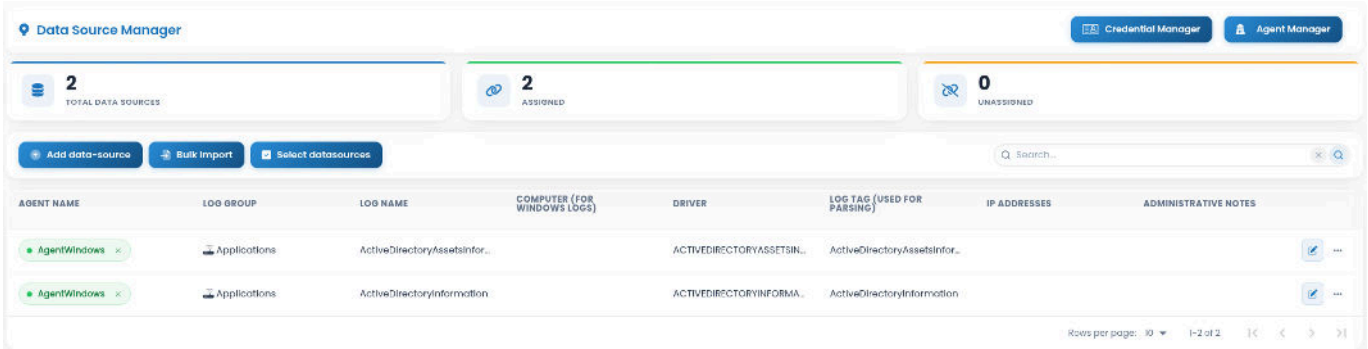
This page describes how to collect events from the Windows Security data source.

Navigate to Settings

Log in to the CYBERQUEST web interface with an account with administrative rights.

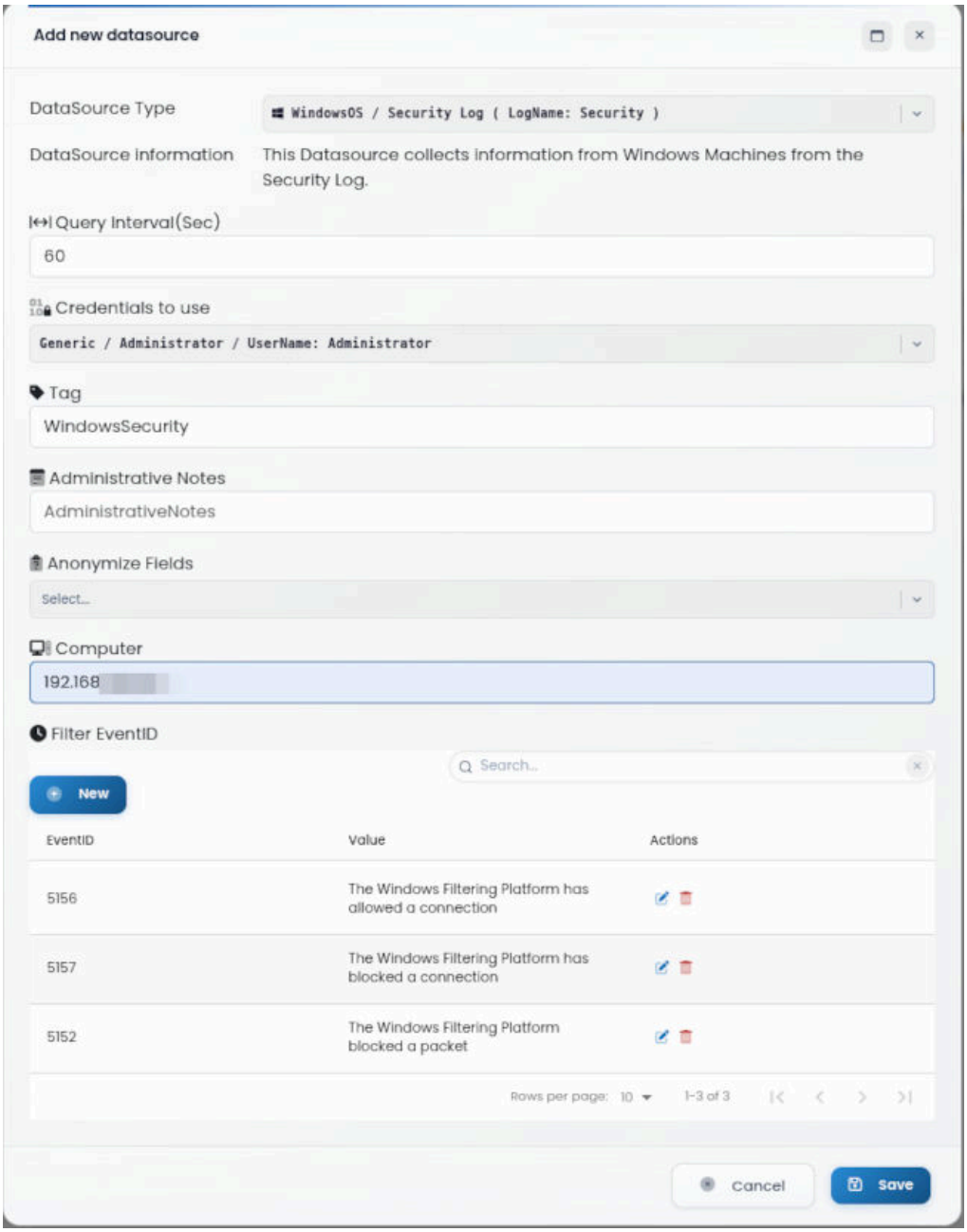
Navigate to “**Settings** > **Management** > **Data Source Manager**”.

This page contains all the data sources added in the CYBERQUEST application.



Complete the form

Press the “ADD DATA-SOURCE” button and complete the following form:

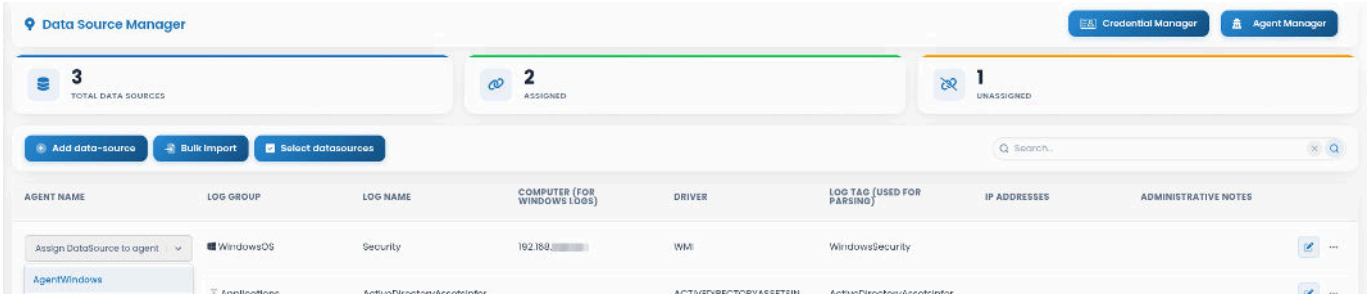


- **DataSource Type:** Select "WindowsOS/ Security Log (LogName: Security)" data source type;
- **DataSource Information:** This field is filled in automatically with data source information;
- **Query Interval:** How often the WMI (Windows Management Instrumentation) query runs. Defaults to every 60 seconds;
- **Credentials to use:** Select a domain or local account with permissions to read the Windows Security log and WMI (See Credential Setup: How to manage Credentials);
- **Tag:** A unique identifier automatically assigned to the data source;
- **Administrative Notes:** Optional notes for administrators;
- **Anonymize Fields:** Select fields to be anonymized. One or more options can be selected;
- **Computer:** Enter the hostname (FQDN) or IP address of the Windows host;

Click the "Save" button to save the data source.

Assign the CYBERQUEST agent

The next step is to assign the CYBERQUEST agent to this data source. Press the drop-down list and choose the agent (often the CQ Server agent).



- **Edit:** Click the

  button to update the data source information. The steps are similar to adding a new data source.

- **Clone:** Click the

  to create a duplicate of the data source.

- **Bulk Clone:** Click the

  to replicate the current data source settings for each entry listed in the **“Bulk Clone”** field.

- **Delete:** To remove a data source, unassign the Agent first, then click **“Delete”**.

Operations · How to collect data on Windows System Log

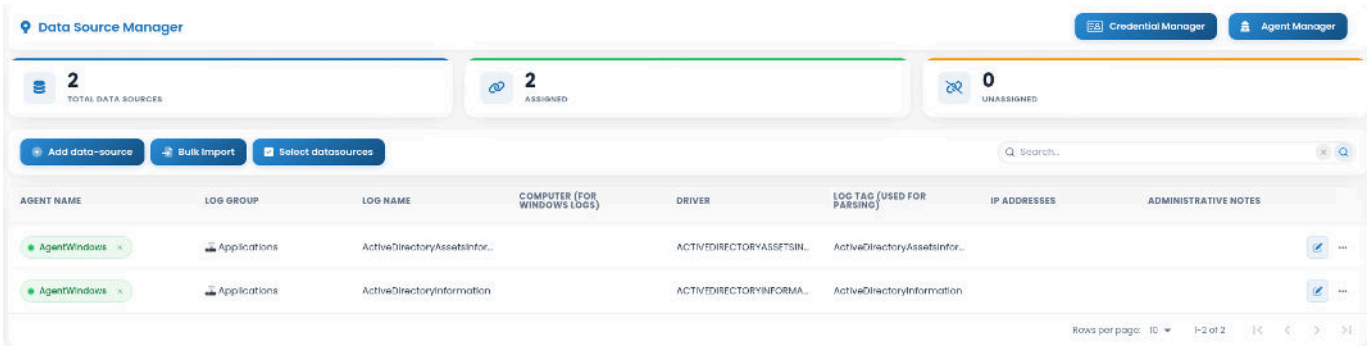
This page describes how to collect events from the Windows System data source.

Navigate to Settings

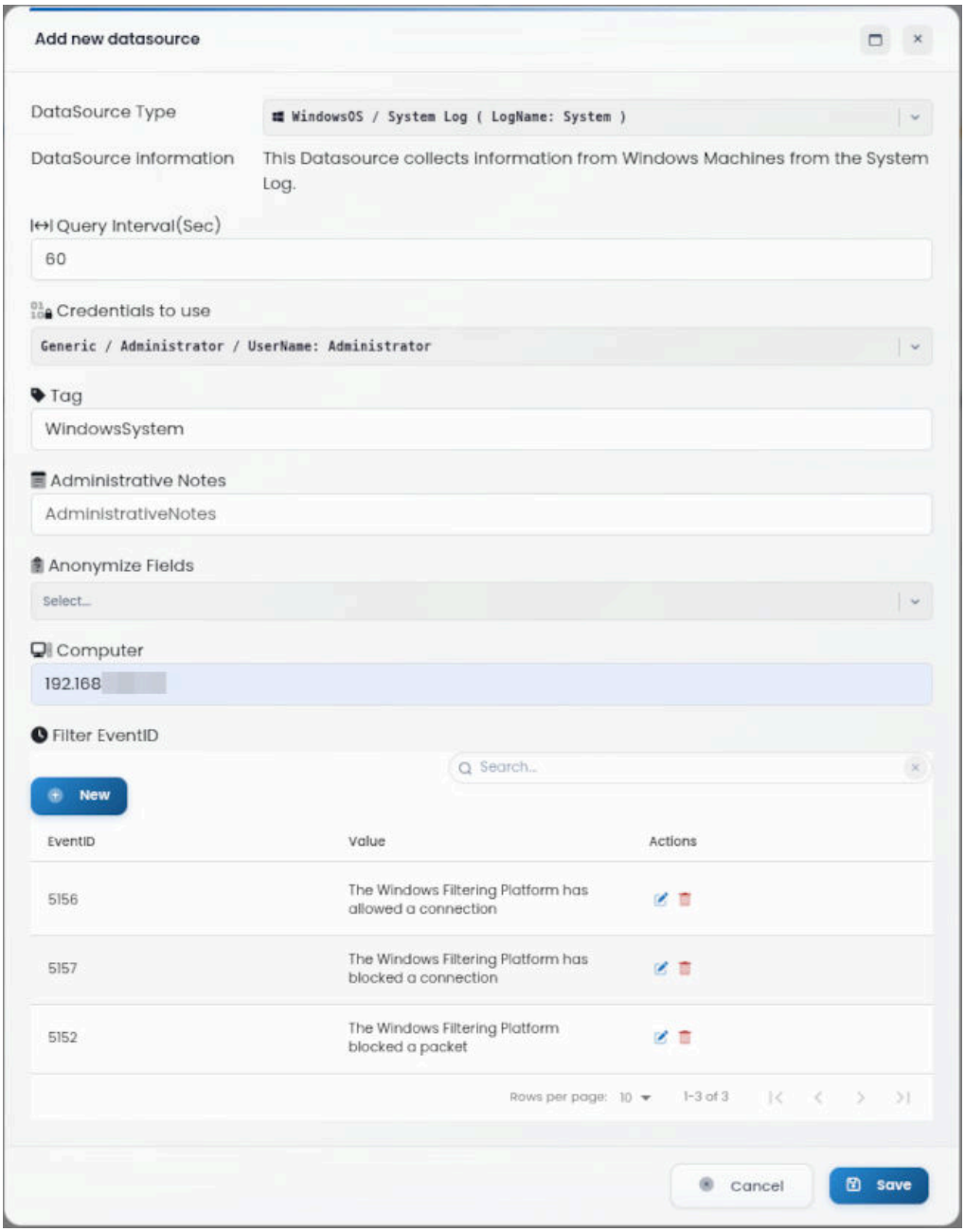
Log in to the CYBERQUEST web interface with an account with administrative rights.

Navigate to “**Settings** > **Management** > **Data Source Manager**”.

This page contains all the data sources added in the CYBERQUEST application.



Press the “Add data-source” button and complete the following form:

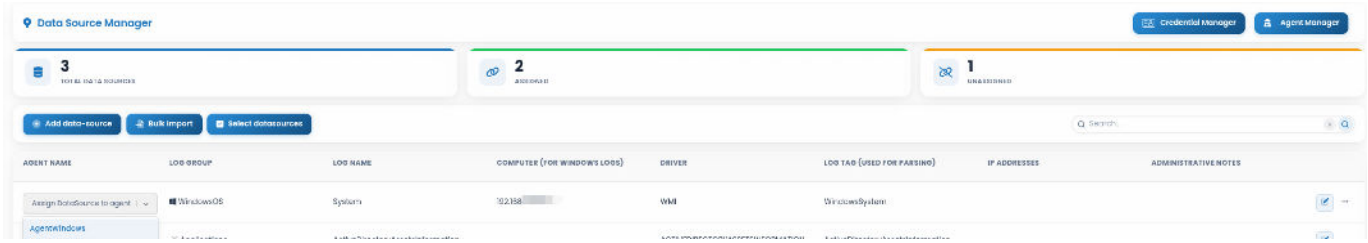


- **DataSource Type:** Select "WindowsOS/ System Log (LogName: System)" data source type;
- **DataSource Information:** This field is filled in automatically with data source information;
- **Query Interval:** How often the WMI (Windows Management Instrumentation) query runs. Defaults to every 60 seconds;
- **Credentials to use:** Select a domain or local account with permissions to read Windows Event Logs and WMI (See Credential Setup: How to manage Credentials);
- **Tag:** A unique identifier automatically assigned to the data source;
- **Administrative Notes:** Optional notes for administrators;
- **Anonymize Fields:** Select fields to be anonymized. One or more options can be selected;
- **Computer:** Enter the hostname (FQDN) or IP address of the Windows host;

Click the "Save" button to save the data source.

Assign the CYBERQUEST agent

The next step is to assign the CYBERQUEST agent to this data source. Press the drop-down list and choose the agent.



- **Edit:** Click the

  button to update the data source information. The steps are similar to adding a new data source.

- **Clone:** Click the

  to create a duplicate of the data source.

- **Bulk Clone:** Click the

  to replicate the current data source settings for each entry listed in the **“Bulk Clone”** field.

- **Delete:** To remove a data source, unassign the Agent first, then click **“Delete”**.

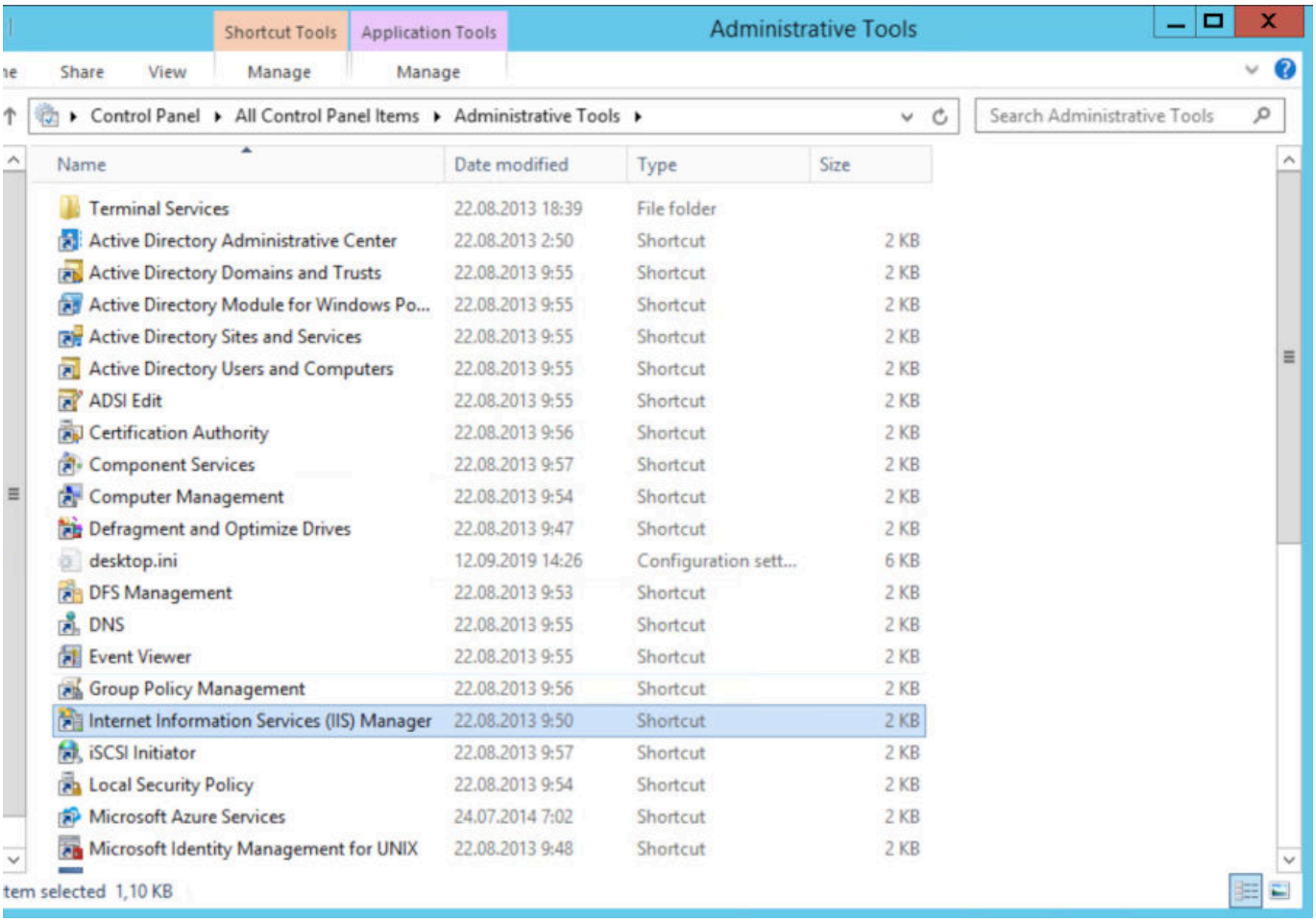
Operations · How to collect IIS Logs with CYBERQUEST

Enable Logging on IIS Server

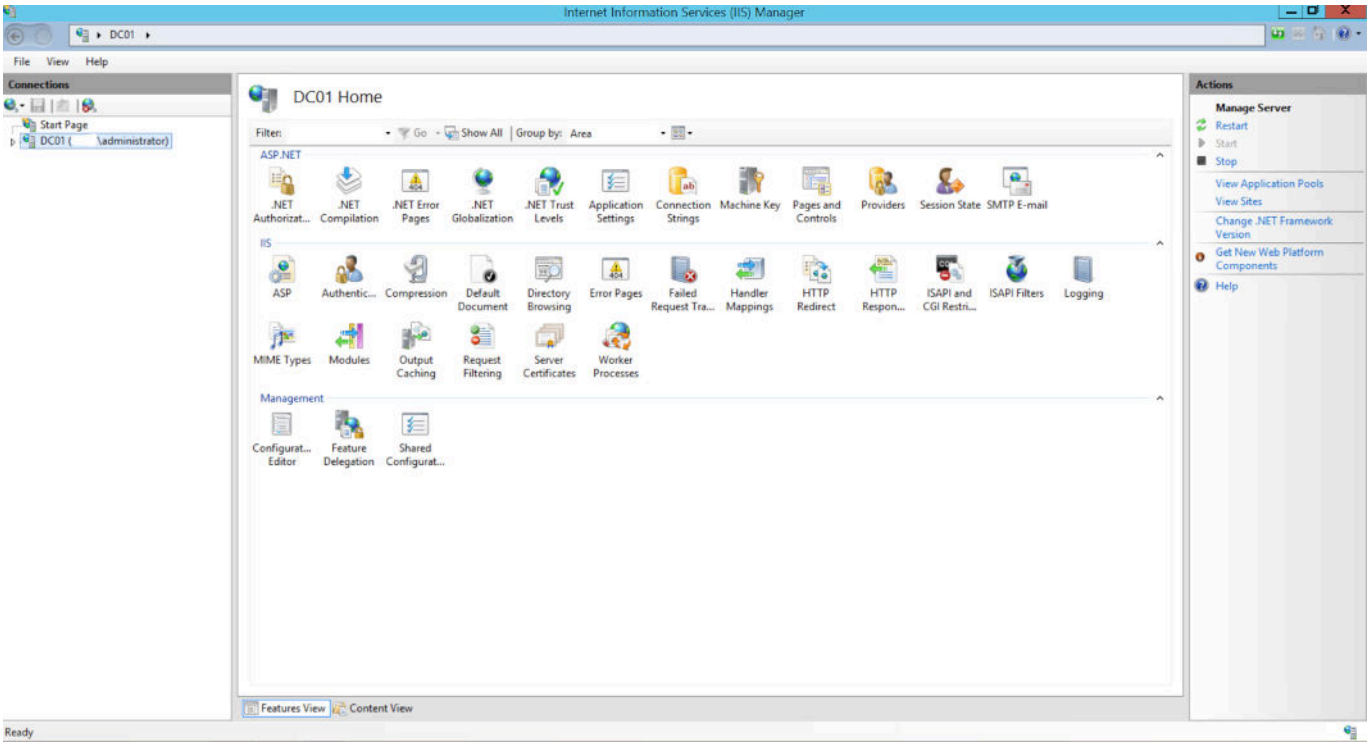
1.Click **Start** and open **Administrative Tools**.



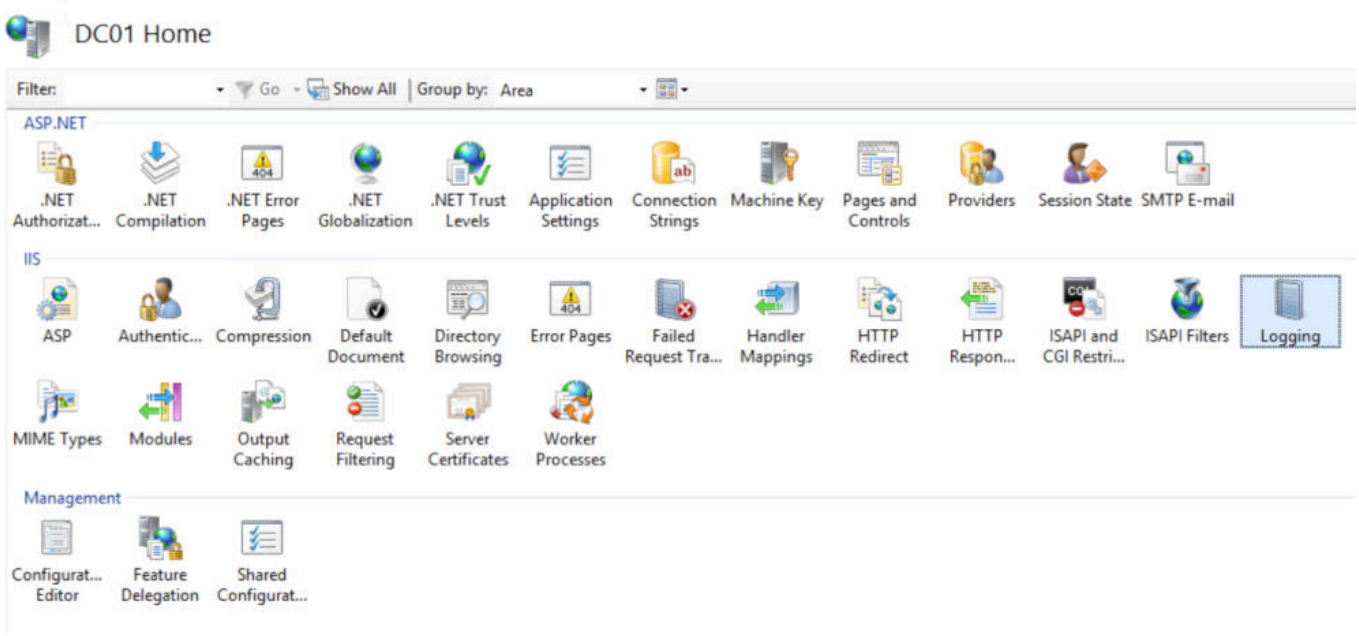
2.Open **Internet Information Services (IIS) Manager**



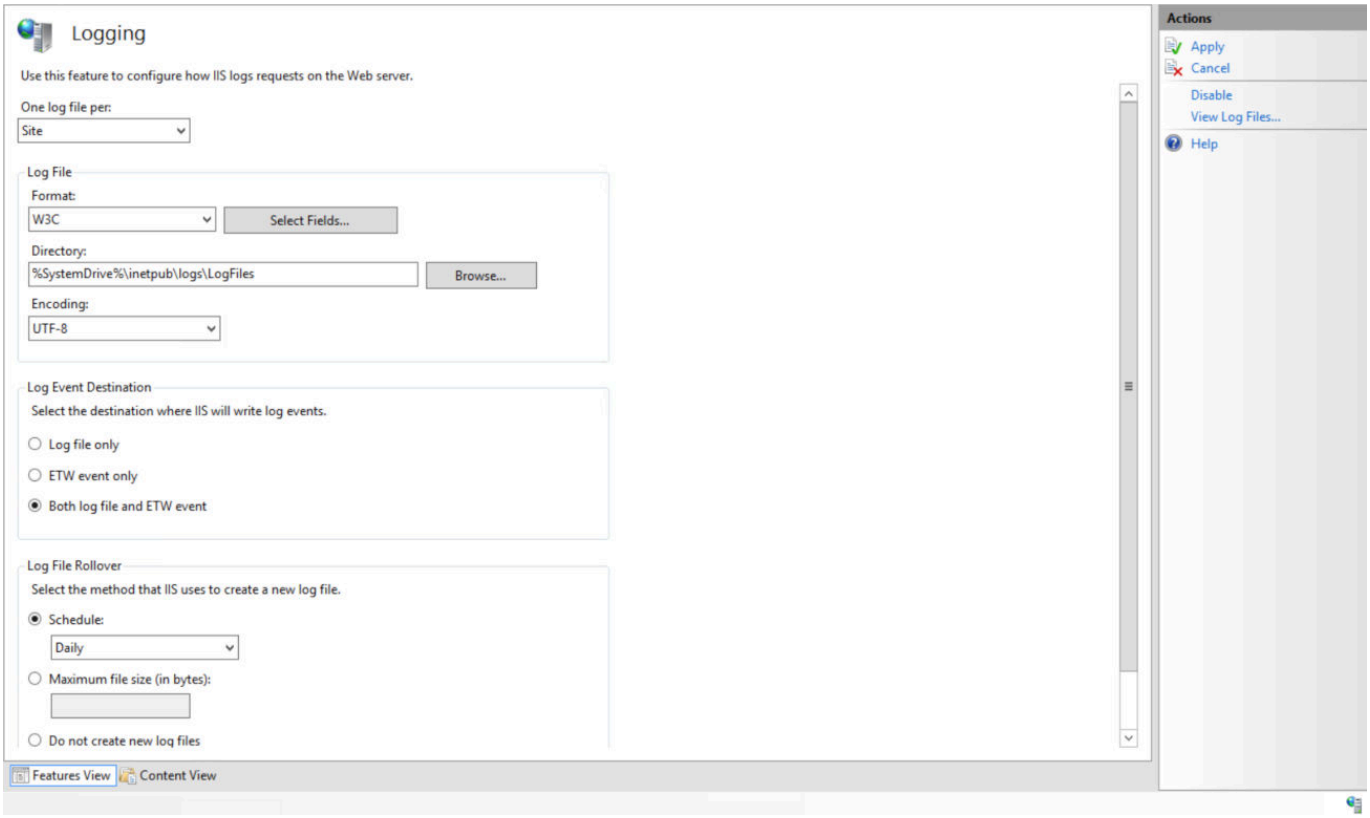
3.In the Top Left corner click once to select the **IIS Server**



4.In the right panel double click on the **Logging** Icon



5.In the **Log Event Destination** click/select **Both log file and ETW event**



6.In the Top Right corner click on **Apply**

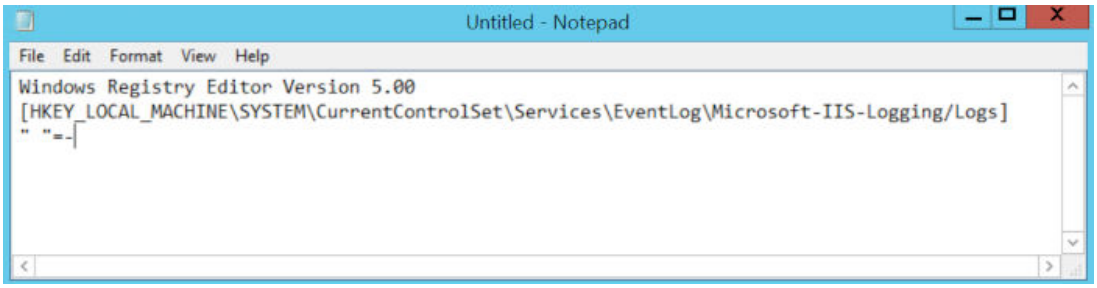
Creating registry key for CQ collection

1.Open a notepad and paste the following script:

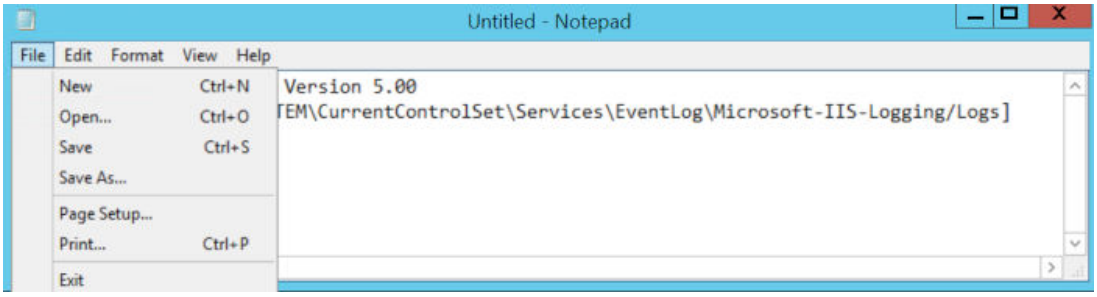
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Microsoft-IIS-Logging/Logs]

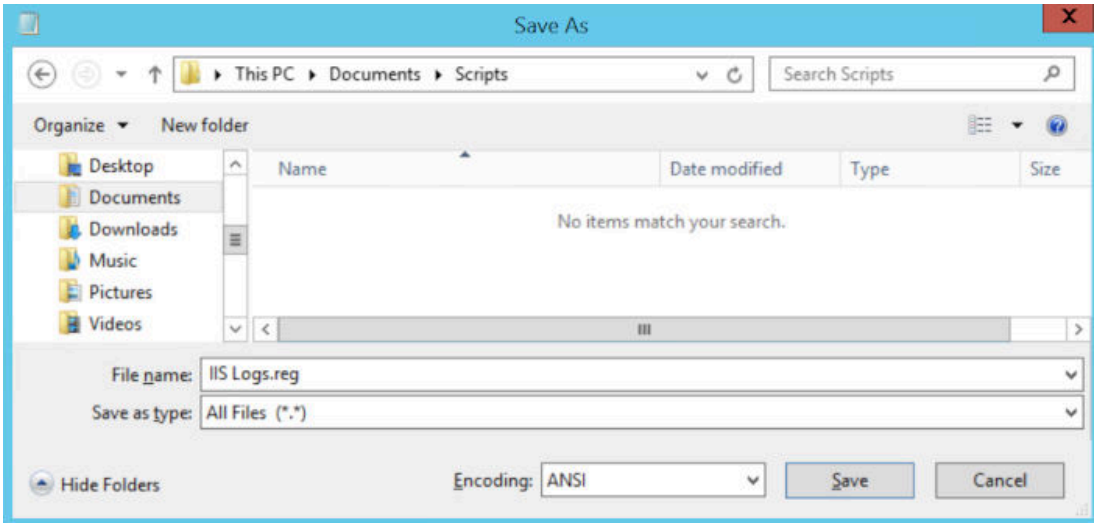
" "=-



2.Click on **File>Save AS...**

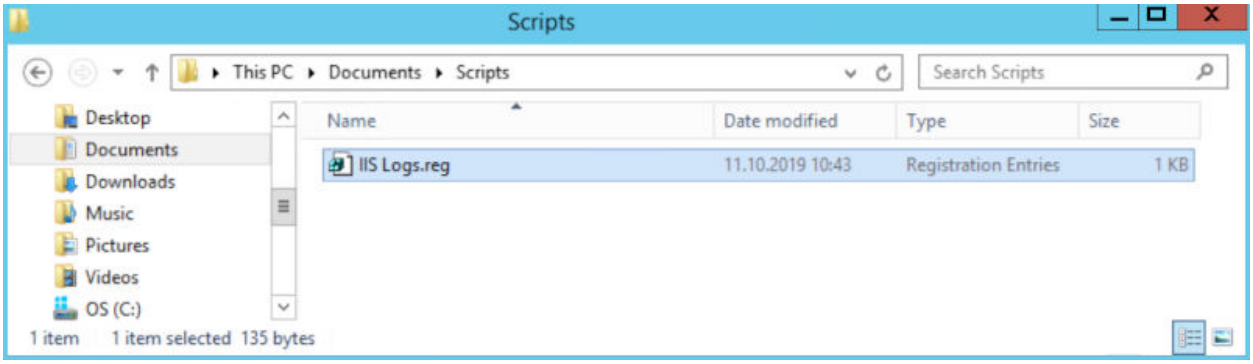


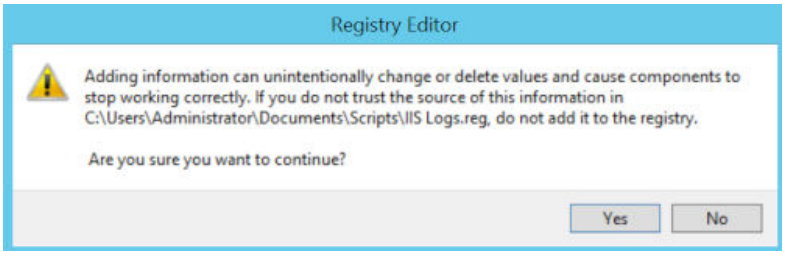
3.Select **All Files (.)** in the **Save as type**



4.In the **File name** section name the file **IIS Logs.reg** and click on **Save**

5.Double Click on the new created file **IIS Logs.reg** and click **Yes**



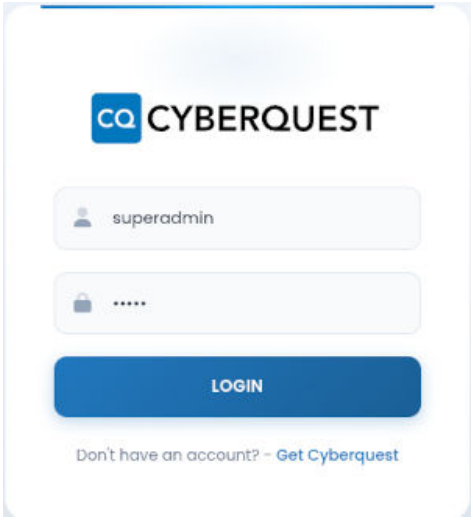


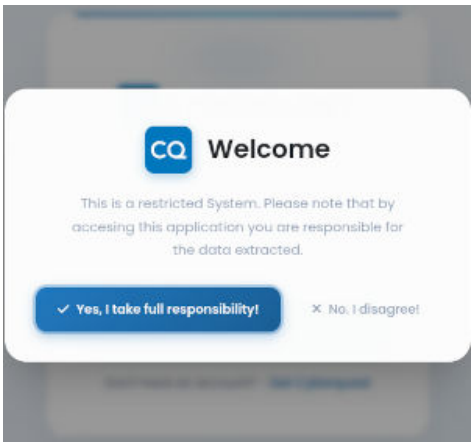
Add new data source

1.Open CYBERQUEST web interface

To access Web Interface, open a web browser and type the application's IP address or DNS name. The default address initially assigned to Web Interface is: ***https://CyberquestIPAddress*** (example).

The browser automatically redirects you to CYBERQUEST's authentication page:



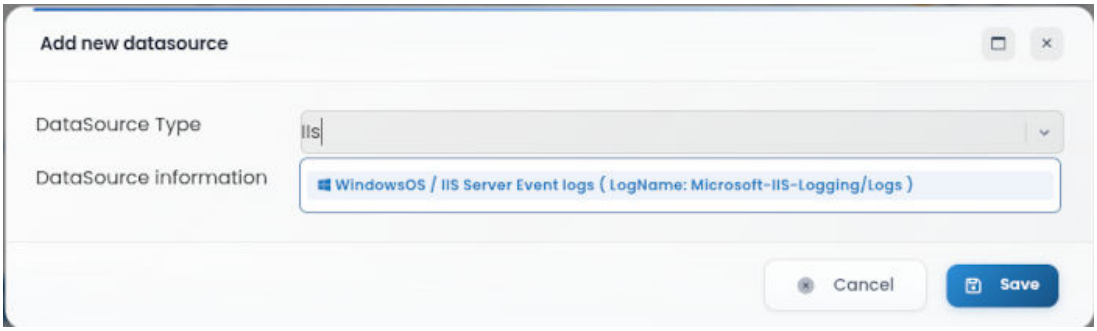


2.**Go to settings > Data Source Manager**

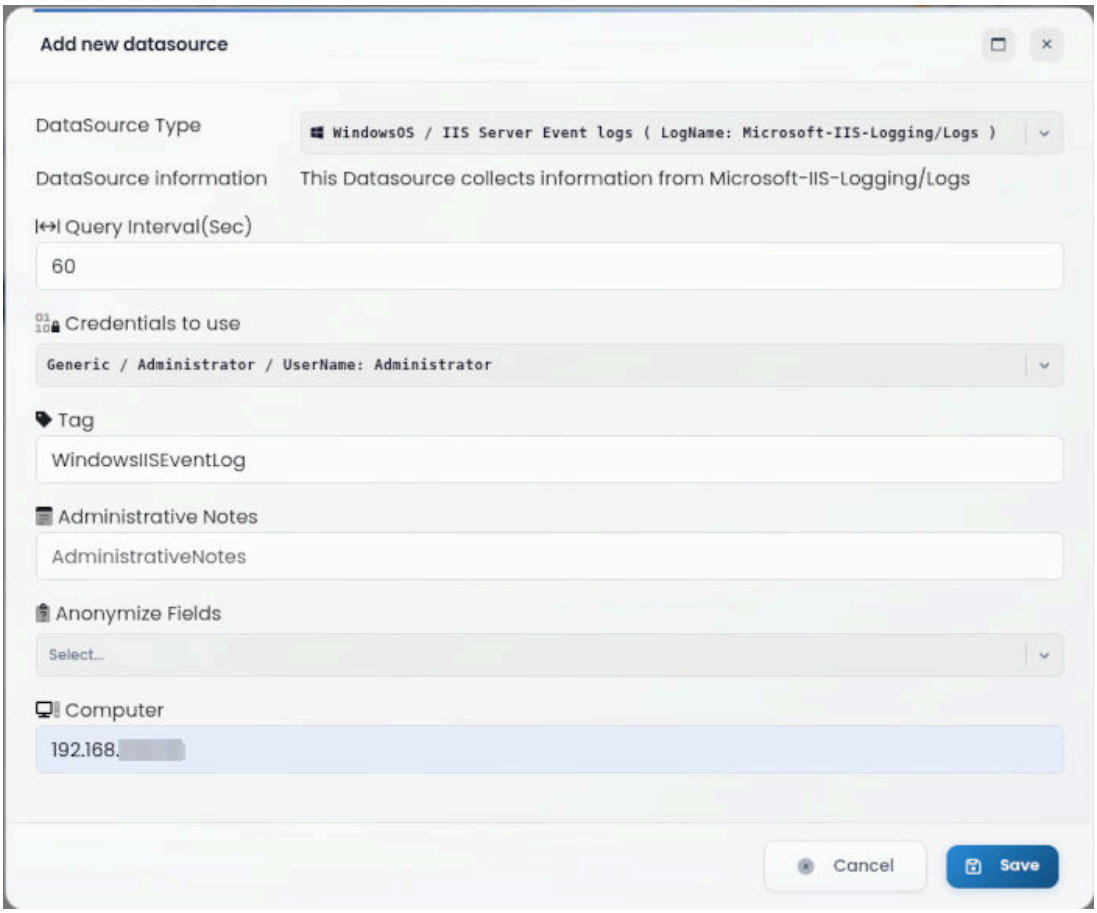
Click on Add Data-Source button



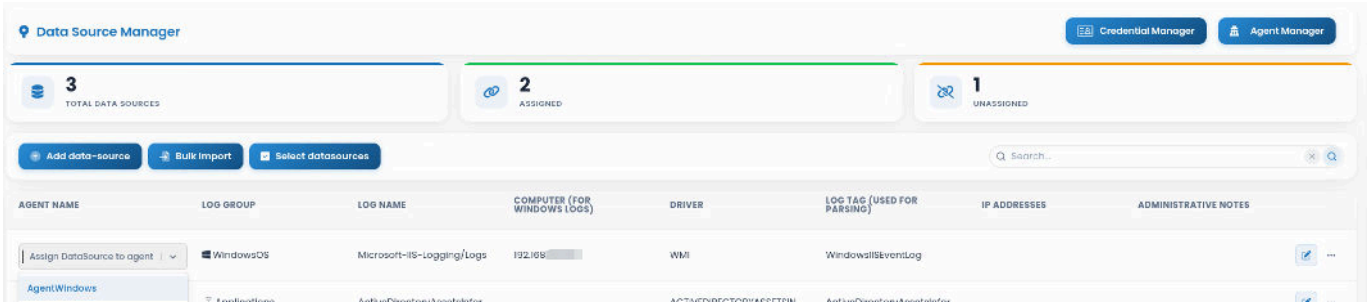
and select DataSource Type: **WindowsOS / IIS Server Event logs**



3.Complete the fields press **Save**



4.Assign DataSource to agent



Operations · How to connect to Active Directory

CYBERQUEST can be integrated with Active Directory or LDAP systems, allowing users to authenticate to CYBERQUEST using their Active Directory credentials. Follow these steps:

Active Directory side

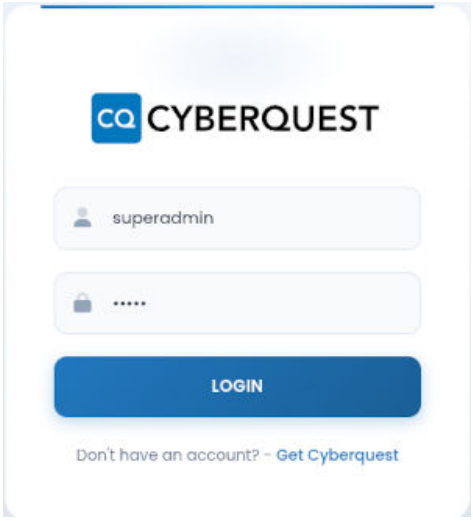
Create the AD group for the CYBERQUEST users (e.g. CQUsers). Add to the AD group the users that will use CYBERQUEST.

CYBERQUEST side

Authentication

To access Web Interface, open a web browser and type the application's address or DNS name. The default address initially assigned to Web Interface is ***https://CyberquestIPAddress*** (example).

The browser automatically redirects you to CYBERQUEST's authentication page:

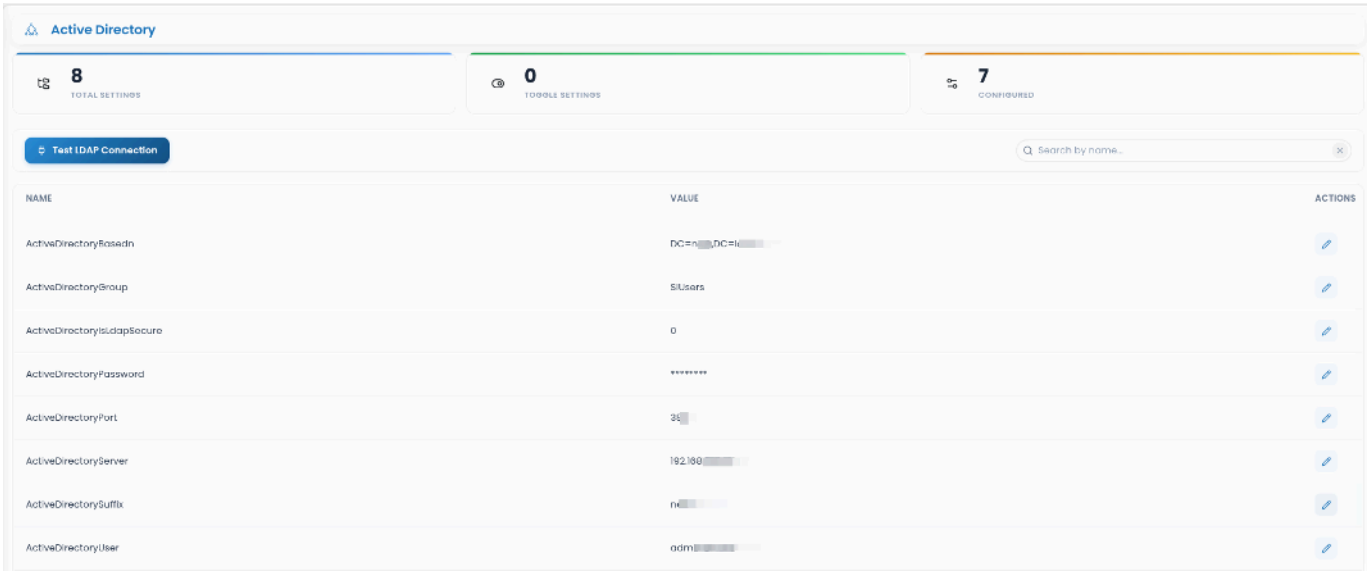


Navigate to Settings

Navigate to "**Settings** > **Application Settings** > **Active Directory**".

Complete the form

Complete the fields with the appropriate information by clicking Edit. The fields are alphabetically ordered:



- **Active Directory Base DN:** Base distinguished name for directory lookups. Example: "CN=Users,DC=domain,DC=com".
- **Active Directory Group:** AD group synchronized with CYBERQUEST.
- **Active Directory Password:** Account password for the mentioned username.
- **Active Directory Port:** Default 389 (LDAP) or 636 (LDAPS; recommended in production).
- **Active Directory Server:** FQDN or IP of a domain controller to query.
- **Active Directory Suffix:** FQDN of the Active Directory domain.
- **Active Directory User:** A dedicated service account with minimal required privileges and read access to the directory (avoid using a Domain Admin account). Example: **domain_name \Administrator**. The default CYBERQUEST account used for collecting events from the Active Directory environment can also be used.

Click Save to apply changes or Close to discard.

After authentication in CYBERQUEST, users must be assigned to the appropriate user groups by a CYBERQUEST administrator.

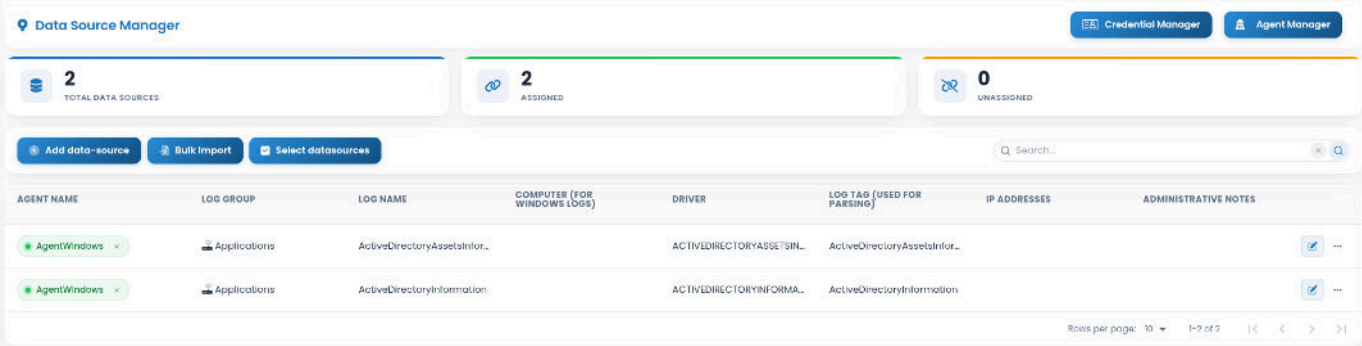
Operations · How to connect to CQ Threat Intelligence

Navigate to Settings

Log in to the CYBERQUEST web interface with an account with administrative rights.

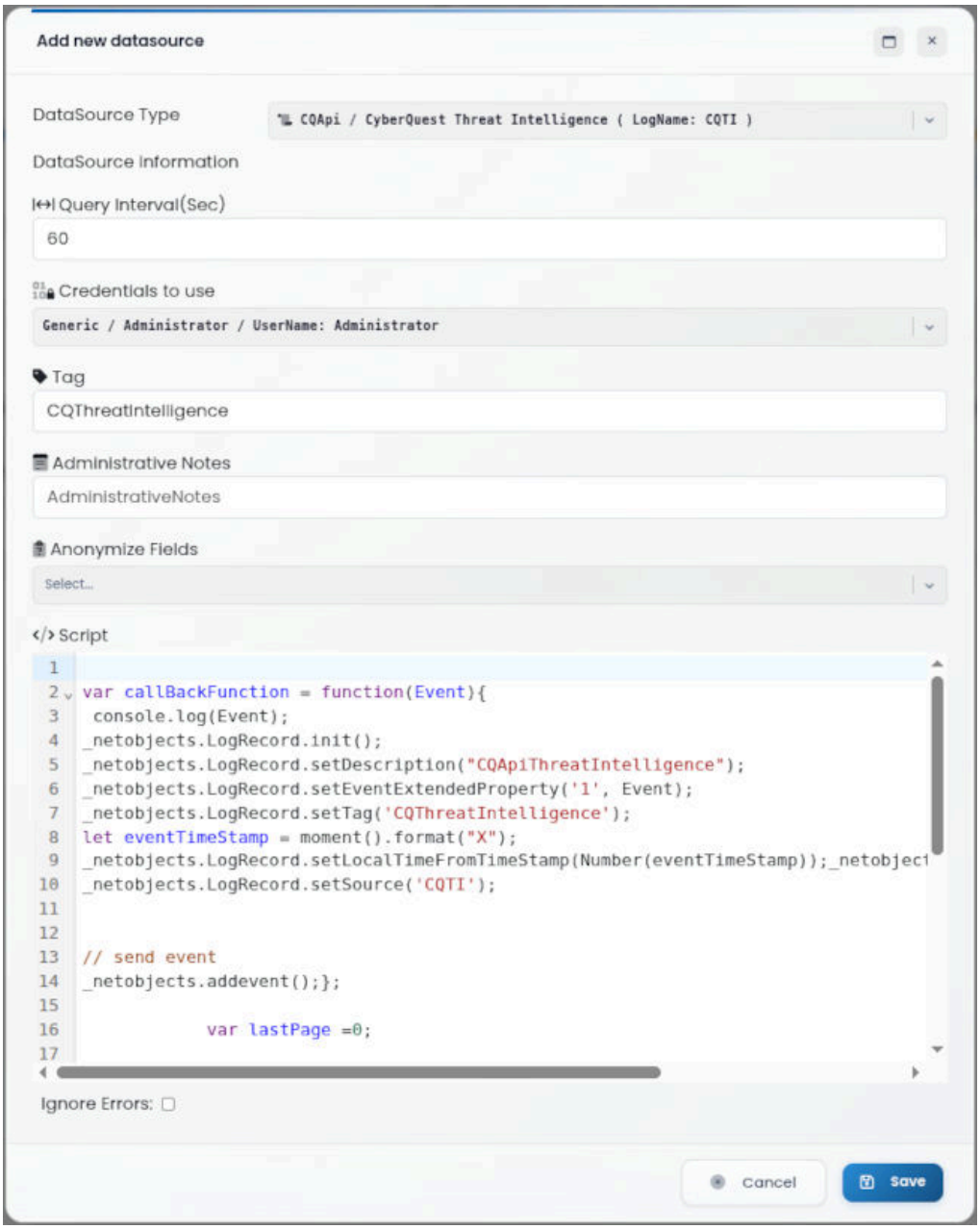
Navigate to **Settings** > **Management** > **Data Source Manager**.

This page contains all the data sources added in the CYBERQUEST application.



Press the “Add data-source” button and complete the following form:

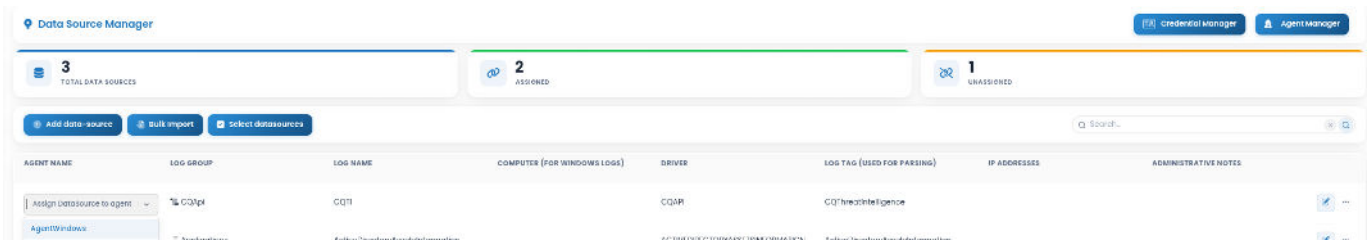
- **DataSource Type:** Select “CQApi / Cyberquest Threat Intelligence (LogName: CQTI)” data source type;
- **DataSource Information:** This field is filled in automatically with data source information;
- **Query Interval:** How often API polling runs. Defaults to every 60 seconds;
- **Credentials to use:** Select appropriate credentials from the drop-down list
- **Tag:** A unique identifier automatically assigned to the data source;
- **Administrative Notes:** Optional notes for administrators;
- **Anonymize Fields:** Select fields to be anonymized. One or more options can be selected;
- **Script:** Configure feed parameters as required;



Click the “Save” button to save the data source.

Assign the CYBERQUEST agent

The next step is to assign the CYBERQUEST agent to this data source. Press the drop-down list and choose the agent.



- **Edit:** Click the



button to update the data source information. The steps are similar to adding a new data source.

- **Clone:** Click the



to create a duplicate of the data source.

- **Delete:** To remove a data source, unassign the Agent first, then click **“Delete”**.

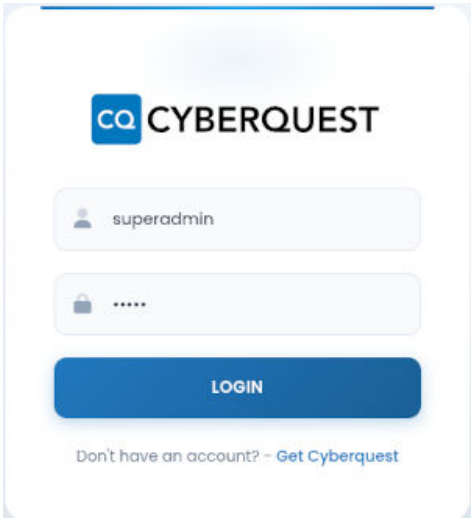
Operations · How to create a Copy job

A Copy job copies data from one data storage path to another. This operation is supported only between offline repositories. Follow the steps below:

Authentication

To access the web interface, open a web browser and type the application’s IP address or DNS name. The default address initially assigned to the web interface is: ***https://CyberquestIPAddress*** (example).

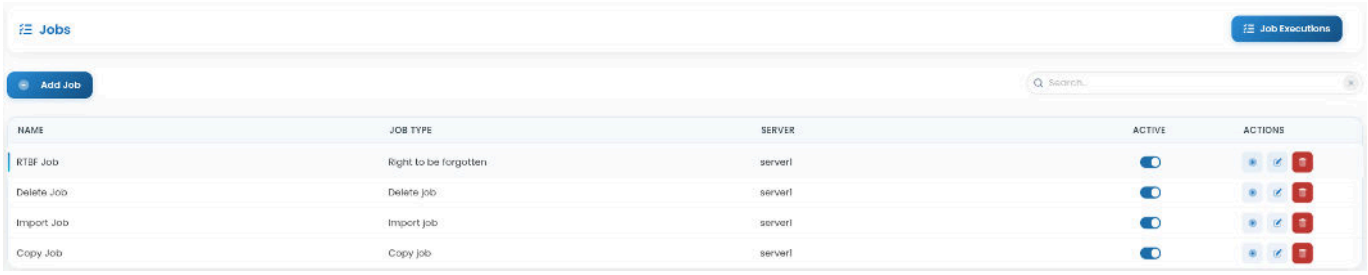
The browser automatically redirects to CYBERQUEST’s authentication page:



Navigate to Settings

Navigate to **Settings > Jobs** and select **Jobs**.

This page contains all types of jobs added in the CYBERQUEST application.



Edit: Click



button to modify a job. The process is similar to adding a new job.

Start Job: Click



button to run the job. The execution status can be monitored on the **Job Executions** page.

Delete: To remove a job from the list, click

button. A confirmation prompt will appear before deletion.

Activate/Deactivate: Use the toggle

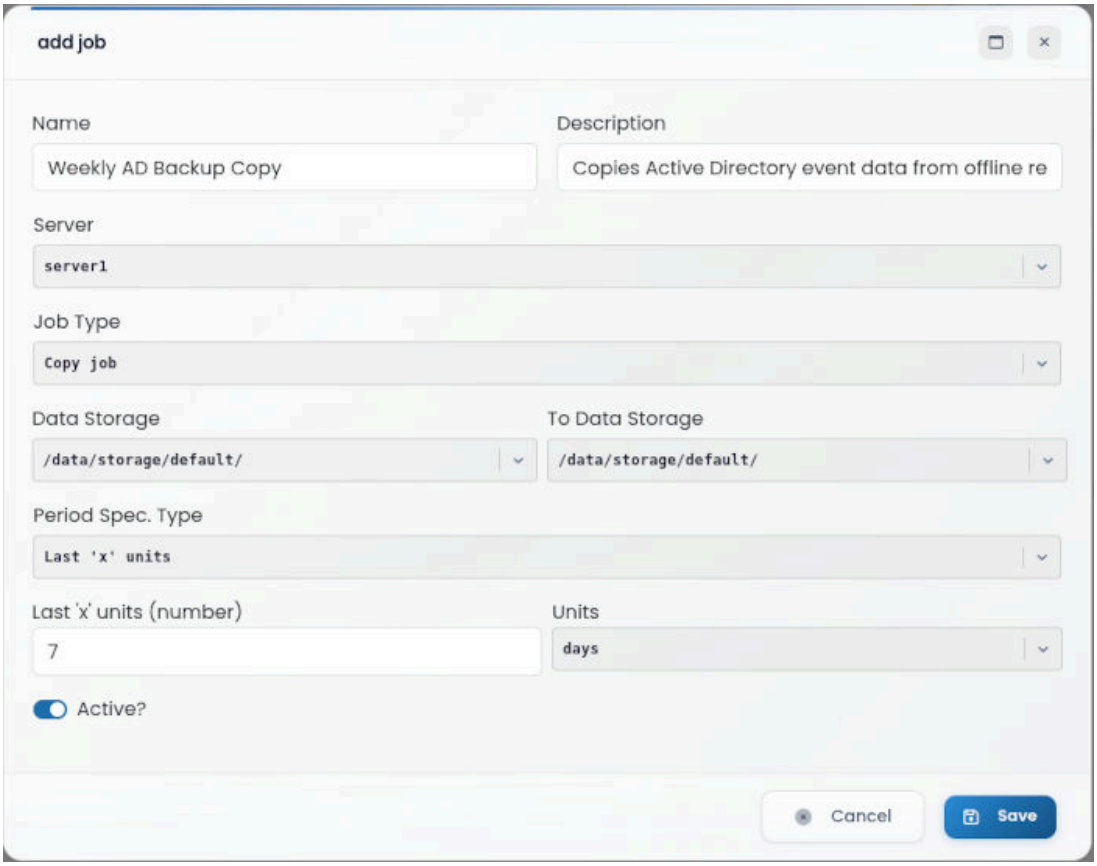
to mark a job as active or inactive.

Create a copy job

To create a copy job, click

Add Job

. A window opens to define a new job.



Job fields:

- **Name:** The display name of the job as it appears in the Jobs list.

  Example: Weekly AD Repository Copy

- **Description:** A short note describing the job's purpose or function.

  Example: Copies Active Directory event data from the offline repository to the backup storage every week

- **Server:** The data server where the job will run.

  Example: server1

- **Job Type:** Select Copy job.

  Copy job: Used to duplicate data between offline repositories: */data/storage/AD_Offline_Repo/* to */data/storage/AD_Backup_Repo/*.

- **Data Storage:** The source storage location (offline) where the data will be copied from.

  Example: /data/storage/AD_Offline_Repo/

- **To Data Storage:** The destination storage where the copied data will be saved.

  Example: /data/storage/AD_Backup_Repo/

- **Period Spec. Type:** Defines the time range of the data to be processed.
  - **Start Date / End Date:** Set a specific time window for data copying.
  - **Last 'x' units:** Define a rolling time frame (e.g., last 7 days, last 24 hours).

    Example: Last 7 days - to copy data from the last week.

- **Active:** Enables or disables the job.

  Example: Set to Active - to start using the job immediately.

When finished, click "Save" to apply changes or "Cancel" to discard.

Verify the job execution

Open **Job Executions** by pressing the



button from the **Jobs** page to confirm the job ran and completed successfully.



Operations · How to create a DTS Alert

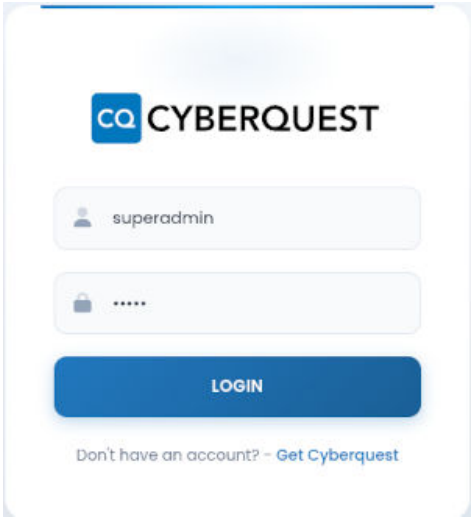
CYBERQUEST alerting is highly customizable per user. Alerts can be defined to respond to specific events, improving accuracy and reducing false positives. Data Transformation Service (DTS) parses data and generates real-time alerts.

Follow the steps to create a new DTS alert:

Authentication

To access the web interface, open a web browser and type the application's address or DNS name. The default address initially assigned to the web interface is: ***https://CyberquestIPAddress*** (example).

The browser automatically redirects to CYBERQUEST's authentication page:

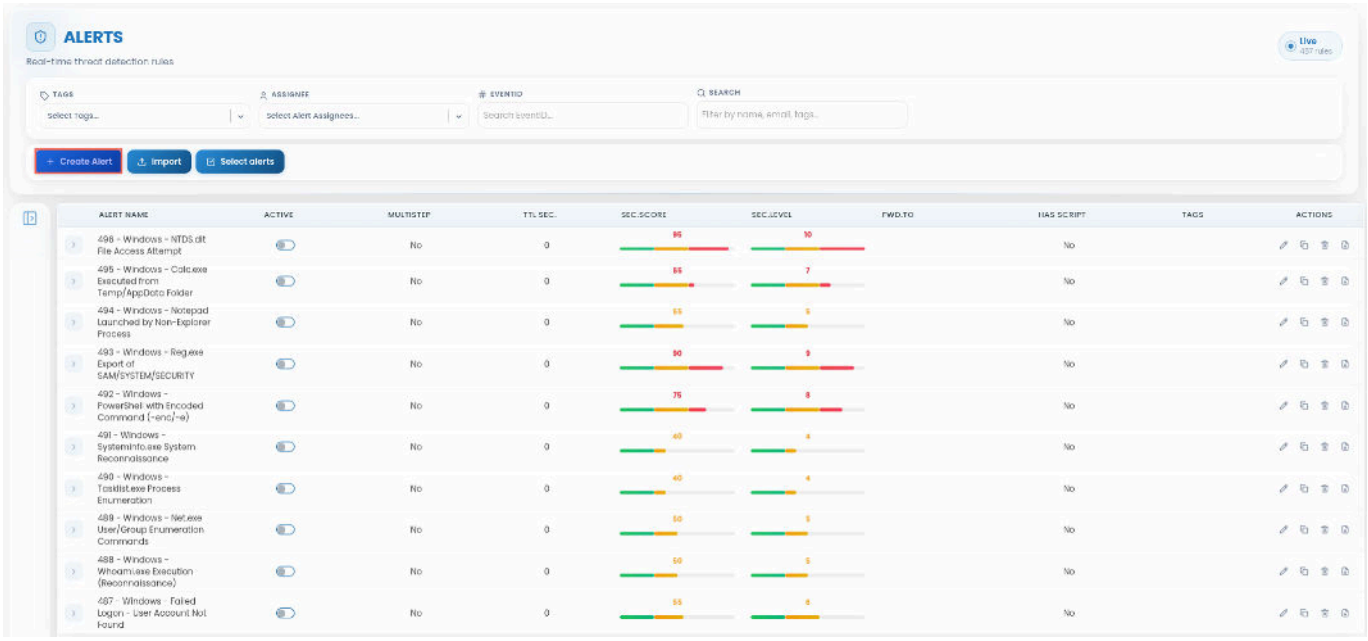


Navigate to Alerts

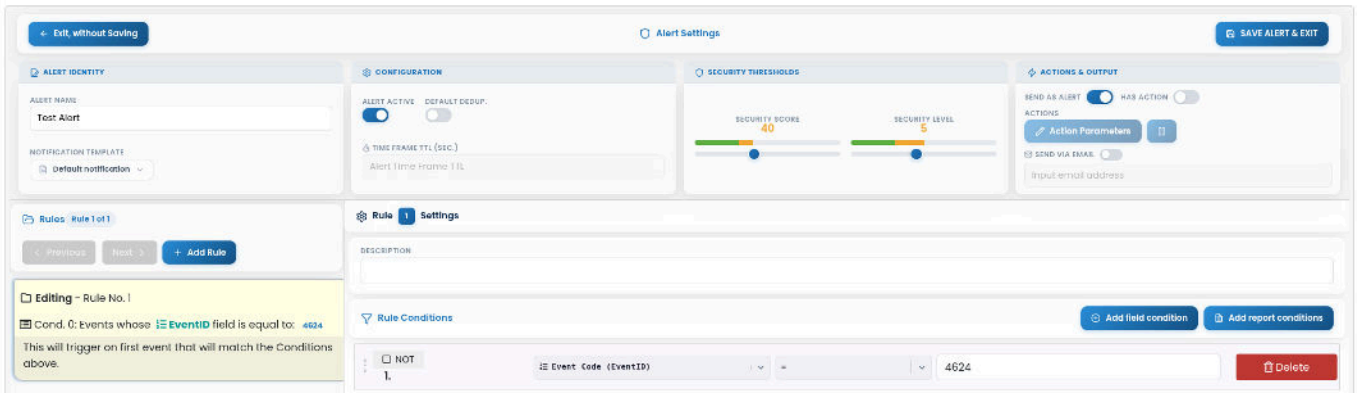
From **Settings**, select **Alerts > Realtime**. The Realtime page opens:

Create new alert definition

On the Alerts page, click **CREATE ALERT** to create a new DTS alert.



The definition form opens.



Alert Name: Name of the new alert.

Alert Active: Select **ALERT ACTIVE** to enable; clear to disable.

Sent as Alert: When cleared, the alert remains active but produces no user-visible notification. Use to correlate anomalies across events, triggers, and alerts.

Has Action: Enable to associate a script executed on trigger. Click **Actions Parameters** to open Script Editor and define the action.

Example: forward alert payload to an HTTP API

```
var httpParameters = {
headers:{
"Content-Type": "application/json",
"Accept": "application/json",
},
};

let requestContent = Event.getAsJSON(Event);
let requestUrl="http://127.0.0.1/myapi";
var output = CQ.Communications.HttpRequest.post(requestUrl, requestContent, httpParameters);
```

The script forwards the alert to another HTTP API.

Notification Template: Select a built-in or custom template. Default is “Default notification”.

Rule Settings defines rule logic using field, report, and correlation conditions joined by AND, OR, and NOT.

Each rule has:

Description: Text describing the rule.

Add field condition: In Select Field, choose an event field; select a value operator; enter the value.

Add report condition: Select a report from existing reports.

Delete: Removes the condition.

When a rule condition is added, a logical operator is automatically added for correlation to the previous condition. The default operator is AND; toggle to OR as needed. Enable NOT to negate a condition when required.

Click **Save** to create the alert.

Operations · How to create a MariaDB cluster for CYBERQUEST operation

Introduction

CYBERQUEST use MariaDB database for solution configuration data.

For architectures High Availability MariaDB nodes are configured in cluster.

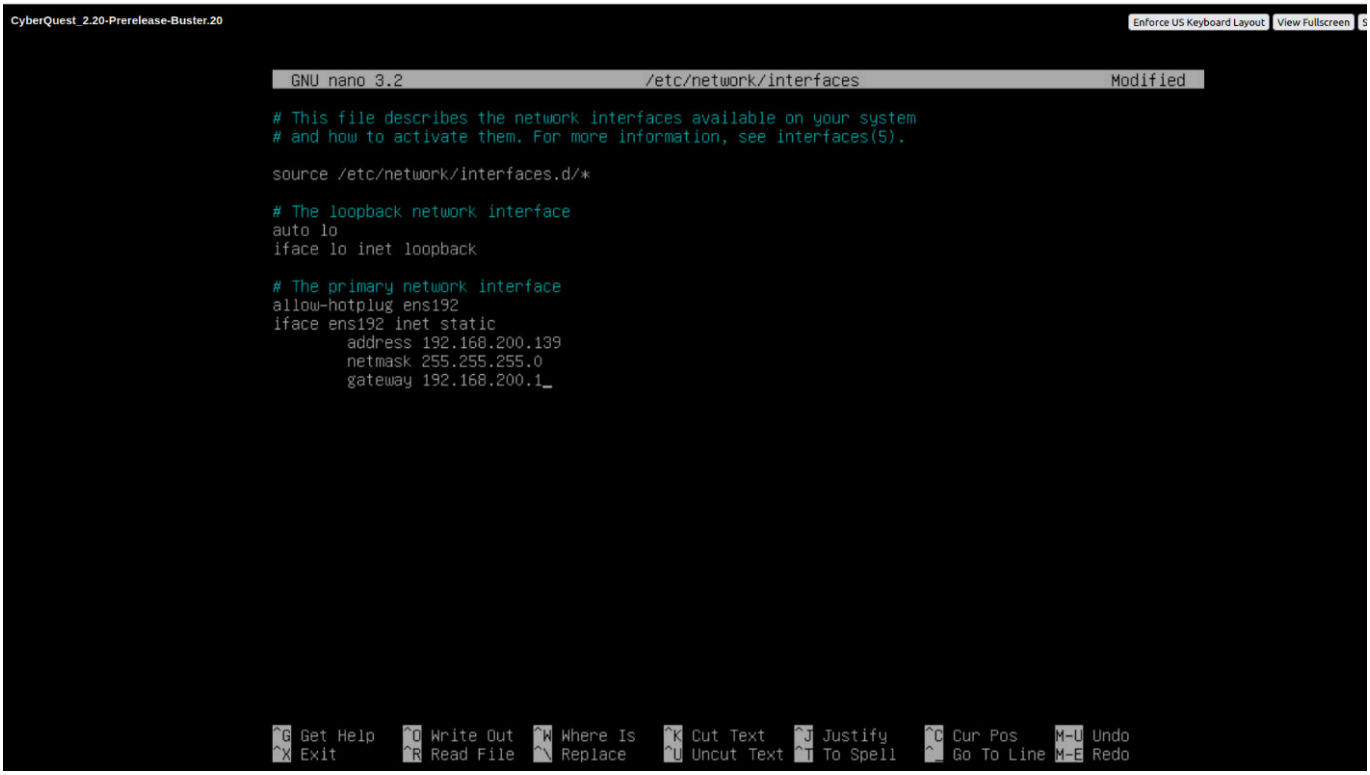
The purpose of this document is to technically describe the MariaDB cluster configuration process.

MariaDB Galera Cluster is used to create the cluster.

Configuring the MariaDB cluster

1.Configuring the network interface

Make sure there are fixed ips on all nodes

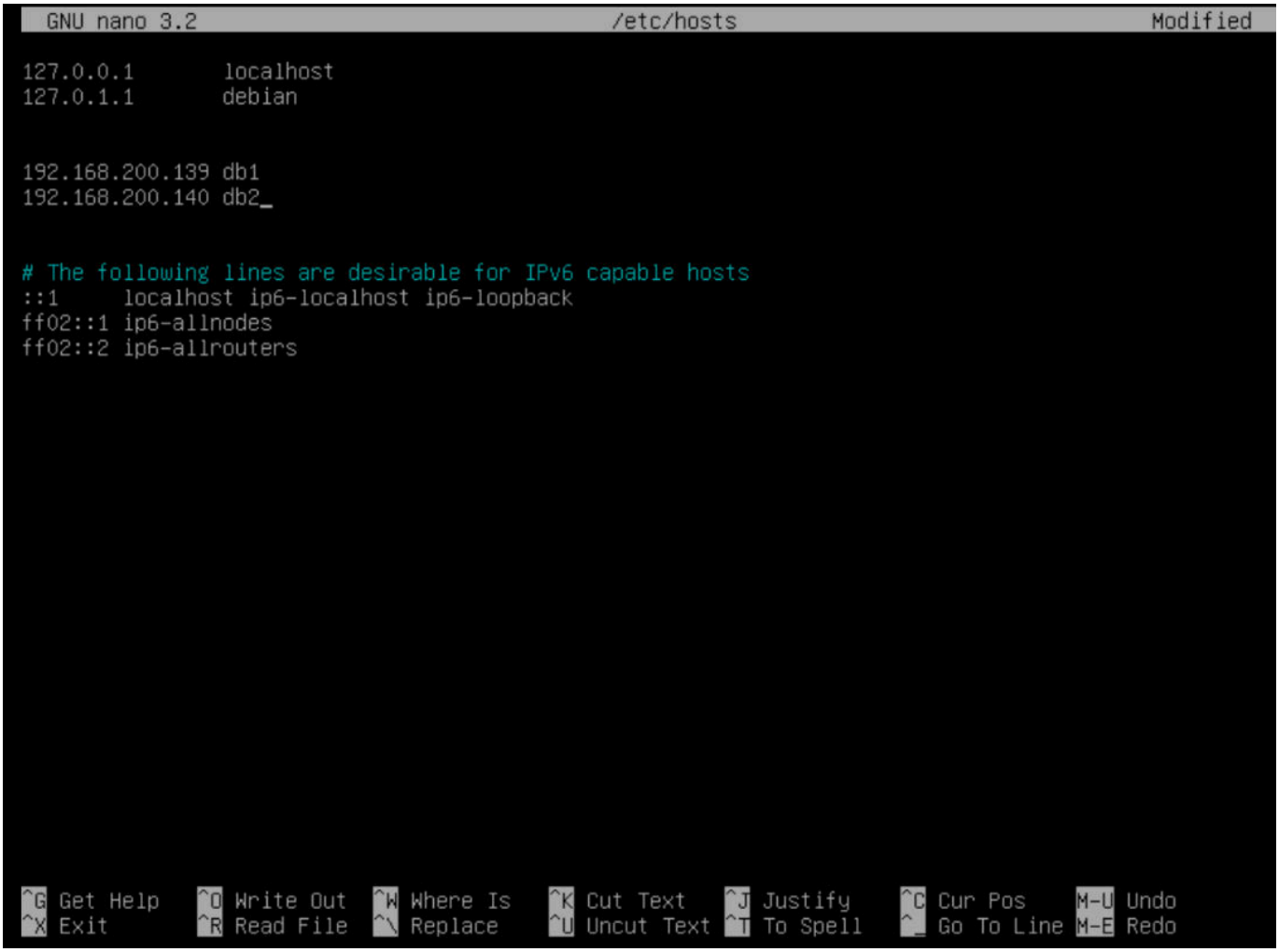



```
ifdown ens192
```

```
ifup ens192
```

Add in **/etc/hosts** node records (on all nodes, in this case db1 and db2)

```
nano /etc/hosts
```



2.Configuring the **60-galera.conf** file

The **60-galera.cnf** clustering configuration file is specific to each node and is created manually - if not found in **/etc/mysql/mariadb.conf.d/**

Configuration file for 192.168.200.139 (db1)

```
# * Galera-related settings
#
# See the examples of server wsrep.cnf files in /usr/share/mysql
# and read more at https://mariadb.com/kb/en/galera-cluster/

[galera]
# Mandatory settings
#wsrep_on = ON
#wsrep_provider =
#wsrep_cluster_address =
#binlog_format = row
#default_storage_engine = InnoDB
#innodb_autoinc_lock_mode = 2

# Allow server to accept connections on all interfaces.
#bind-address = 0.0.0.0

# Optional settings
#wsrep_slave_threads = 1
#innodb_flush_log_at_trx_commit = 0


[mysqld]
binlog_format=ROW
default-storage-engine=innodb
innodb_autoinc_lock_mode=2
bind-address=0.0.0.0

# Galera Provider Configuration
wsrep_on=ON
wsrep_provider=/usr/lib/galera/libgalera_smm.so

# Galera Cluster Configuration
wsrep_cluster_name="CQ_CLUSTER"
wsrep_cluster_address="gcomm://192.168.200.139,192.168.200.140"

# Galera Synchronization Configuration
wsrep_sst_method=rsync

# Galera Node Configuration
wsrep_node_address="192.168.200.139"
wsrep_node_name="db1"
```

Configuration file for 192.168.200.140 (db2)

```
# * Galera-related settings
#
# See the examples of server wsrep.cnf files in /usr/share/mysql
# and read more at https://mariadb.com/kb/en/galera-cluster/

[galera]
# Mandatory settings
#wsrep_on = ON
#wsrep_provider =
#wsrep_cluster_address =
#binlog_format = row
#default_storage_engine = InnoDB
#innodb_autoinc_lock_mode = 2

# Allow server to accept connections on all interfaces.
#bind-address = 0.0.0.0

# Optional settings
#wsrep_slave_threads = 1
#innodb_flush_log_at_trx_commit = 0


[mysqld]
binlog_format=ROW
default-storage-engine=innodb
innodb_autoinc_lock_mode=2
bind-address=0.0.0.0

# Galera Provider Configuration
wsrep_on=ON
wsrep_provider=/usr/lib/galera/libgalera_smm.so

# Galera Cluster Configuration
wsrep_cluster_name="CQ_CLUSTER"
wsrep_cluster_address="gcomm://192.168.200.139,192.168.200.140"

# Galera Synchronization Configuration
wsrep_sst_method=rsync

# Galera Node Configuration
wsrep_node_address="192.168.200.140"
wsrep_node_name="db2"
```

3.Final configuration

Copy the configuration file to **/home/superadmin** on both nodes

```
vlad@vlad-HP-ZBook-17-G2:~$
vlad@vlad-HP-ZBook-17-G2:~$
vlad@vlad-HP-ZBook-17-G2:~$
vlad@vlad-HP-ZBook-17-G2:~$
vlad@vlad-HP-ZBook-17-G2:~$ scp 60-galera.cnf superadmin@192.168.200.139:~/
superadmin@192.168.200.139's password:
60-galera.cnf                                 100%  960   779.0KB/s   00:00
vlad@vlad-HP-ZBook-17-G2:~$ scp 60-galera.cnf superadmin@192.168.200.140:~/
The authenticity of host '192.168.200.140 (192.168.200.140)' can't be established.
ECDSA key fingerprint is SHA256:rle4tJ5s9gRVFxVgJIpNJQ3j5rEZamdckkXD4fUjOW8.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.200.140' (ECDSA) to the list of known hosts.
superadmin@192.168.200.140's password:
60-galera.cnf                                 100%  960   831.0KB/s   00:00
vlad@vlad-HP-ZBook-17-G2:~$
```

Stop Mariadb services on both nodes

```
superadmin@debian:~$
superadmin@debian:~$ sudo systemctl stop mariadb.service
[sudo] password for superadmin:
superadmin@debian:~$
```

Copy the configuration file to each node separately

```
sudo cp /home/superadmin/60-galera.cnf /etc/mysql/mariadb.conf.d/
```

Cluster verification

1.Checking the configurations

Check the configuration in the file (on each node)

```
  GNU nano 3.2                /etc/mysql/mariadb.conf.d/60-galera.cnf                 Modified

#
# * Galera-related settings
#
# See the examples of server wsrep.cnf files in /usr/share/mysql
# and read more at https://mariadb.com/kb/en/galera-cluster/

[galera]
# Mandatory settings
#wsrep_on = ON
#wsrep_provider =
#wsrep_cluster_address =
#binlog_format = row
#default_storage_engine = InnoDB
#innodb_autoinc_lock_mode = 2

# Allow server to accept connections on all interfaces.
#bind-address = 0.0.0.0

# Optional settings
#wsrep_slave_threads = 1
#innodb_flush_log_at_trx_commit = 0


[mysqld]
binlog_format=ROW
default-storage-engine=innodb
innodb_autoinc_lock_mode=2
bind-address=0.0.0.0

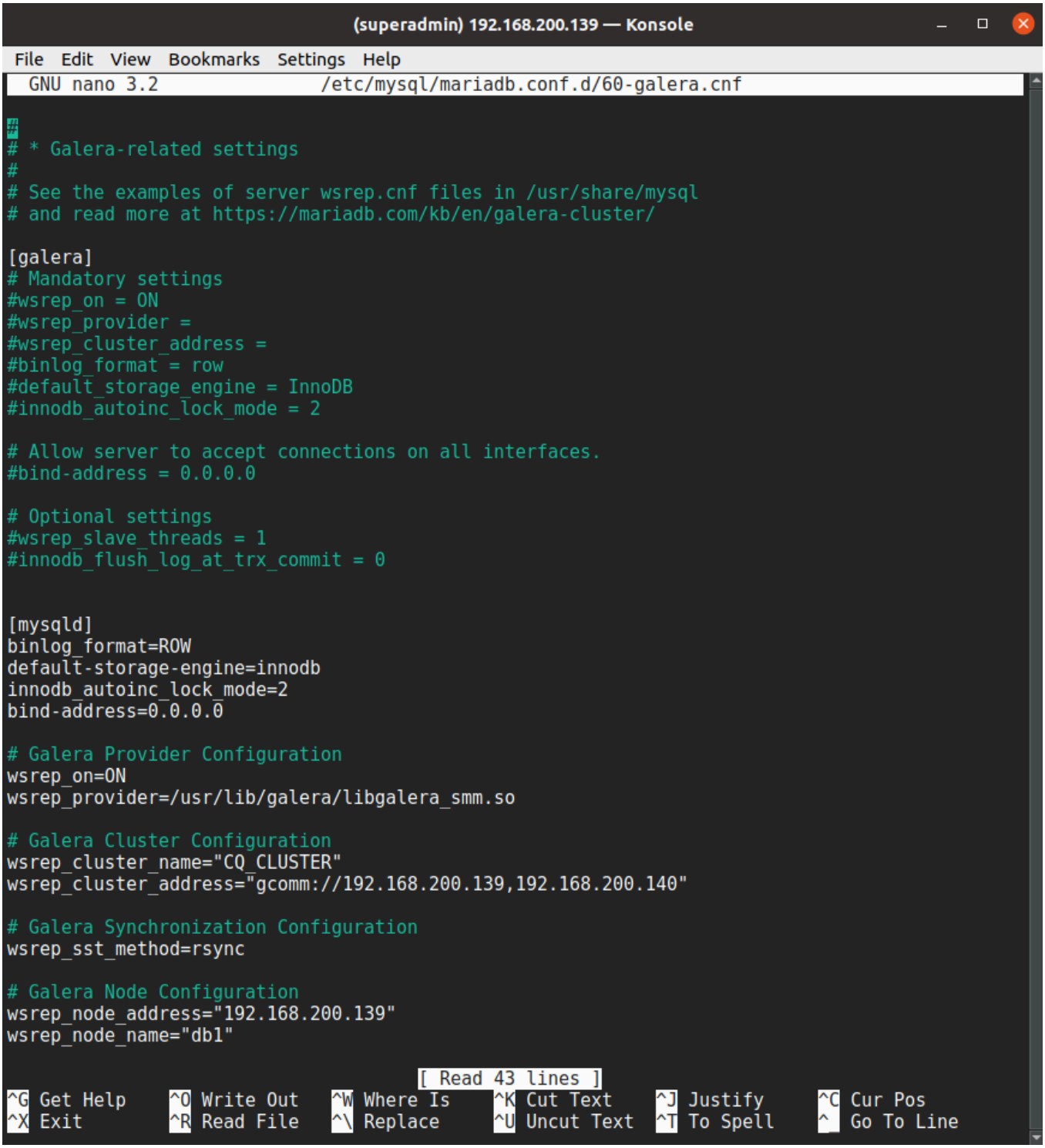
# Galera Provider Configuration
wsrep_on=ON
wsrep_provider=/usr/lib/galera/libgalera_smm.so

# Galera Cluster Configuration
wsrep_cluster_name="CQ_CLUSTER"
wsrep_cluster_address="gcomm://192.168.200.139,192.168.200.140"

# Galera Synchronization Configuration
wsrep_sst_method=rsync

# Galera Node Configuration
wsrep_node_address="192.168.200.140"
wsrep_node_name="db2"

^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos
^X Exit        ^R Read File   ^\ Replace     ^U Uncut Text  ^T To Spell    ^_ Go To Line
```



Make bootstrap of new cluster (on db1)

```
sudo galera_new_cluster
```

```
superadmin@debian:~$ sudo galera_new_cluster
superadmin@debian:~$ systemctl status ma
machine.slice    man-db.service   man-db.timer     mariadb.service
superadmin@debian:~$ systemctl status mariadb.service
● mariadb.service - MariaDB 10.3.27 database server
   Loaded: loaded (/lib/systemd/system/mariadb.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2021-06-18 12:53:22 EEST; 25s ago
     Docs: man:mysqld(8)
           https://mariadb.com/kb/en/library/systemd/
  Process: 25531 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d /var/run/mysqld (cod
  Process: 25532 ExecStartPre=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (co
  Process: 25534 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ] && VAR= ||   VAR=`c
  Process: 25691 ExecStartPost=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (c
  Process: 25693 ExecStartPost=/etc/mysql/debian-start (code=exited, status=0/SUCCESS)
 Main PID: 25655 (mysqld)
   Status: "Taking your SQL requests now..."
    Tasks: 42 (limit: 4700)
   Memory: 117.0M
   CGroup: /system.slice/mariadb.service
           └─25655 /usr/sbin/mysqld --wsrep-new-cluster --wsrep_start_position=00000000-0000-0
lines 1-16/16 (END)
```

Starting the service on db2 (which is already configured):

```
sudo systemctl start mariadb.service
```

Verify that the database status has been received

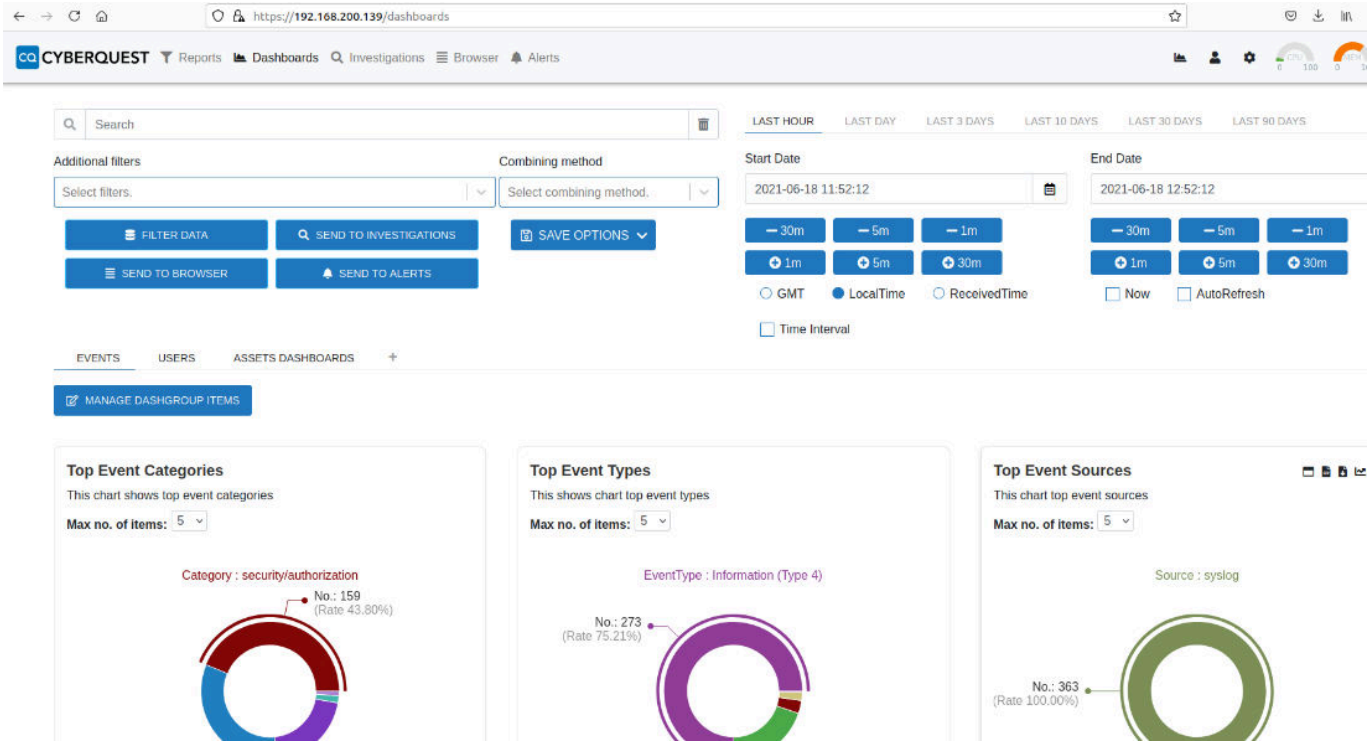
```
uperadmin@debian:~$ sudo systemctl status mariadb.service
sudo] password for superadmin:
● mariadb.service - MariaDB 10.3.27 database server
   Loaded: loaded (/lib/systemd/system/mariadb.service; enabled; vendor preset: enabled)
   Active: inactive (dead) since Fri 2021-06-18 12:34:08 EEST; 21min ago
     Docs: man:mysqld(8)
           https://mariadb.com/kb/en/library/systemd/
  Process: 630 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d /var/run/mysqld (code=
  Process: 663 ExecStartPre=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code
● mariadb.service - MariaDB 10.3.27 database server
   Loaded: loaded (/lib/systemd/system/mariadb.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2021-06-18 12:56:11 EEST; 7s ago
     Docs: man:mysqld(8)
           https://mariadb.com/kb/en/library/systemd/
  Process: 4289 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d /var/run/mysqld (code=exited, status=0/SU
  Process: 4290 ExecStartPre=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=exited, status=0/S
  Process: 4292 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ] && VAR= ||   VAR=`cd /usr/bin/..; /usr/b
  Process: 4565 ExecStartPost=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=exited, status=0/
  Process: 4567 ExecStartPost=/etc/mysql/debian-start (code=exited, status=0/SUCCESS)
 Main PID: 4413 (mysqld)
   Status: "Taking your SQL requests now..."
    Tasks: 42 (limit: 4700)
   Memory: 291.4M
   CGroup: /system.slice/mariadb.service
           └─4413 /usr/sbin/mysqld --wsrep_start_position=00000000-0000-0000-0000-000000000000:-1

un 18 12:56:09 debian rsyncd[4507]: sent 1739 bytes  received 1225280 bytes  total size 1218647
un 18 12:56:09 debian rsyncd[4504]: sent 2708 bytes  received 7942426 bytes  total size 7930277
un 18 12:56:09 debian rsyncd[4516]: connect from db1 (192.168.200.139)
un 18 12:56:09 debian rsyncd[4516]: rsync to rsync_sst/ from db1 (192.168.200.139)
un 18 12:56:09 debian rsyncd[4516]: receiving file list
un 18 12:56:09 debian rsyncd[4516]: sent 48 bytes  received 185 bytes  total size 41
un 18 12:56:10 debian rsyncd[4470]: sent 0 bytes  received 0 bytes  total size 0
un 18 12:56:11 debian systemd[1]: Started MariaDB 10.3.27 database server.
un 18 12:56:11 debian /etc/mysql/debian-start[4569]: Upgrading MySQL tables if necessary.
un 18 12:56:11 debian /etc/mysql/debian-start[4583]: Checking for insecure root accounts.
```

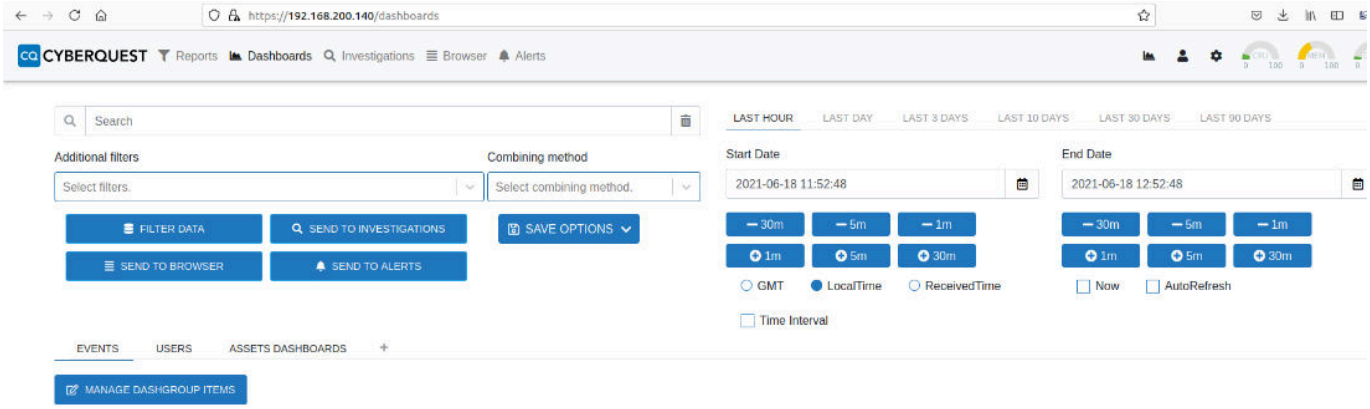
2.Check GUI

Check the replication when accessing the web interface. The configurations must be identical for the two CYBERQUEST machines.

db1:



db2:



You can see the identical configuration of dashgroups: Events, Users, Asset Dashboards.

Operations · How to create new alerts

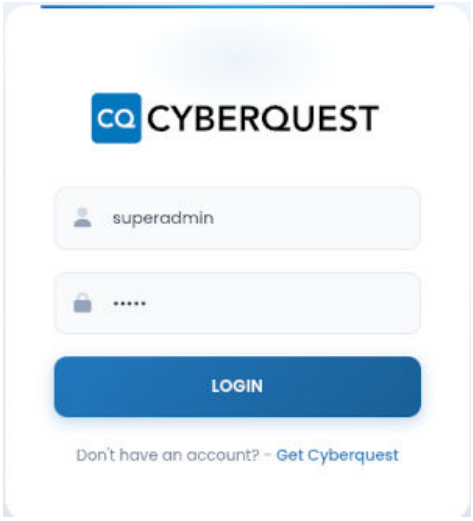
CYBERQUEST alerting is highly customizable per user. Alerts can be defined to respond to specific events, improving accuracy and reducing false positives.

Follow the steps to create a new alert:

Step 1. Authentication

To access the web interface, open a browser and enter the application's IP address or DNS name. The default address initially assigned to the web interface is ***https://CyberquestIPAddress*** (example).

The browser automatically redirects to CYBERQUEST's authentication page:

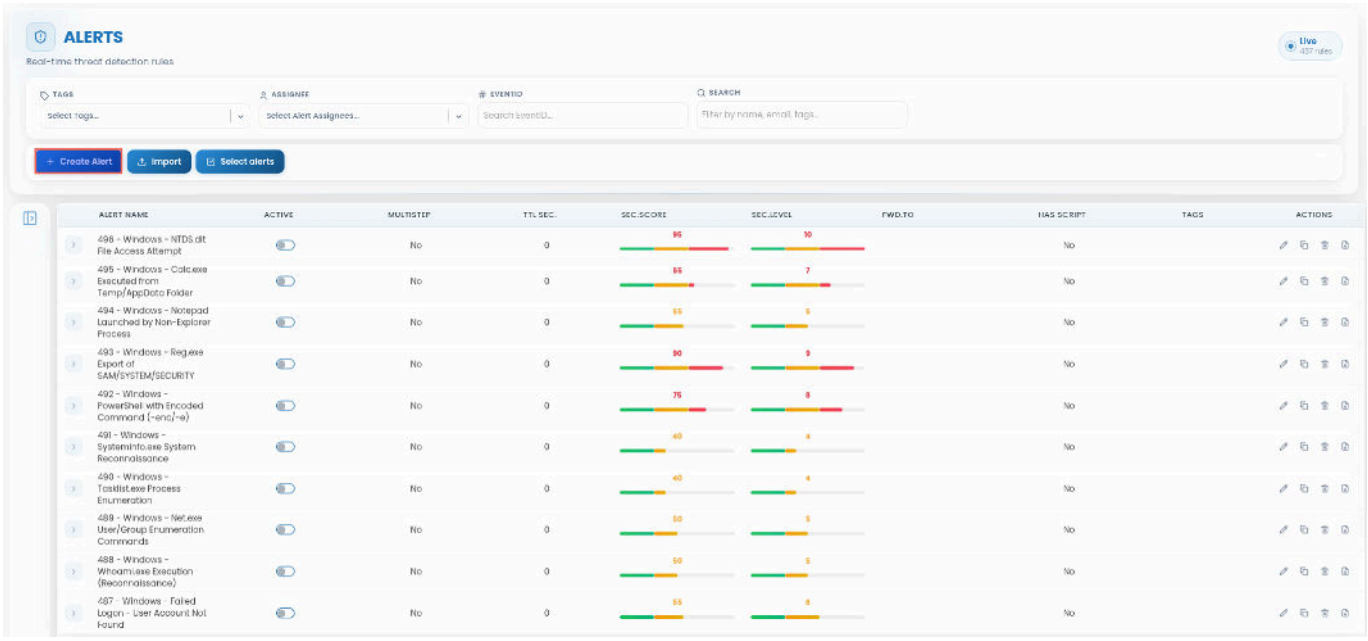


Step 2. Navigate to Alerts

From **Settings**, select **Alerts > Realtime**. The Realtime page opens.

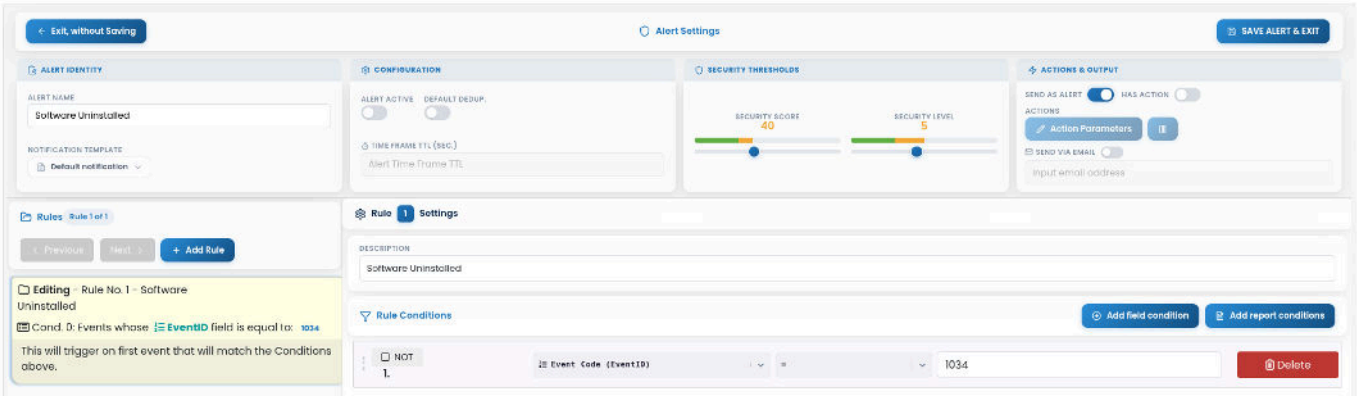
Step 3. Create new alert definition

On the Alerts page, click **Create new alert definition** to create a new alert.



Step 4. Complete the form

Complete the form and click “Save Alert & Exit”:



- **Alert Name:** Name of the new alert.

- **Alert Active:** Select **ALERT ACTIVE** to enable and clear to disable.
- **Time Frame TTL (sec):** Duration the alert remains active after triggering.
- **Alert Security Score:**Reference score used for dynamic scoring. The real-time score adjusts between this value and 100, depending on rules and event volume.
- **Alert Security Level:** Behaves similarly to score, uses the same color coding.
- **Sent as Alert:** When cleared, the alert remains active but produces no user-visible notification, used for backend correlation across events, triggers, and alerts.
- **Has Action:** Enable to associate a script executed on trigger. Click **Actions Parameters** to open Script Editor and define the action.
- **Send via Email:** Enable to send the alert to defined recipients.
- **Notification Template:** Select a built-in or custom template. Default is “Default notification”.

Under Rules, define logic using field, report, and correlation conditions joined by AND, OR, and NOT. Supports single-event rules and complex correlations (event order, or missing events in a sequence).

- **Previous / Next:** Navigate between rule conditions.
- **Add Rule:** Adds a new rule. Configure it in the Rule Settings pane.

Rule Settings defines rule logic:

- **Description:** Text describing the rule.
- **Add field condition:** Select an event field, a value operator, and a value.
- **Add report condition:** Select a report from existing reports.
- **Delete:** Removes the condition.

When a condition is added, AND is the default operator; toggle to OR as needed. Enable NOT to negate a condition when required.

Operations · How to create a new report and how to run

How to create a new report and run it

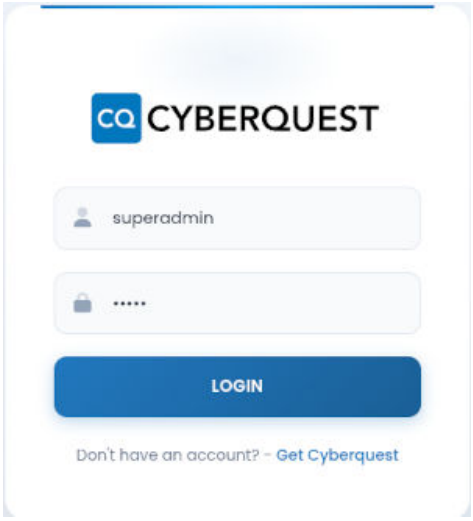
The module enables both scheduled and ad hoc reporting, either collectively or in detail, to provide a comprehensive compliance and operational overview. The interface displays only the reports authorized for each user. Through a simple web-based interface, predefined and customizable reports can be accessed quickly to deliver immediate insights.

How to create a new report

Authentication

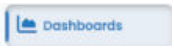
To access the web interface, open a browser and enter the application’s IP address or DNS name. The default address initially assigned to the web interface is ***https://CyberquestIPAddress*** (example).

The browser automatically redirects to CYBERQUEST’s authentication page:

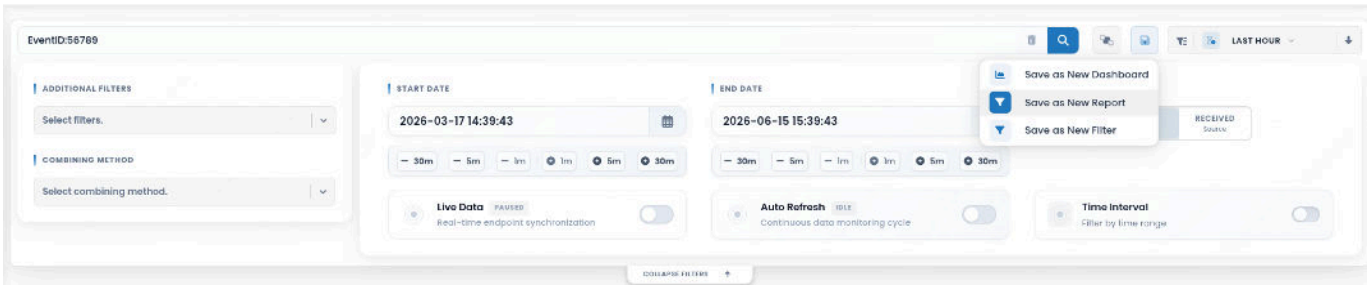


Navigate to Dashboards

From the left navigation, open the Dashboards module (or click the Dashboards icon):



Apply a filter for the data of interest (for example: `EventID:"56789"`). Save it as a report: click **SAVE OPTIONS** > **Save as New Report**.



Complete the form

Complete the form and click “Next”.

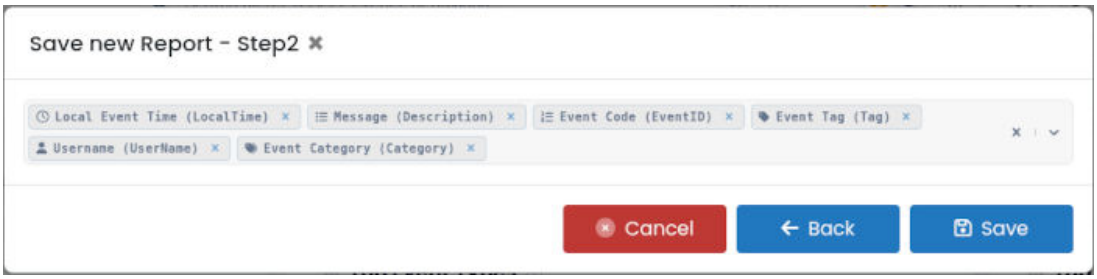
Name: Report name

Description: Short description

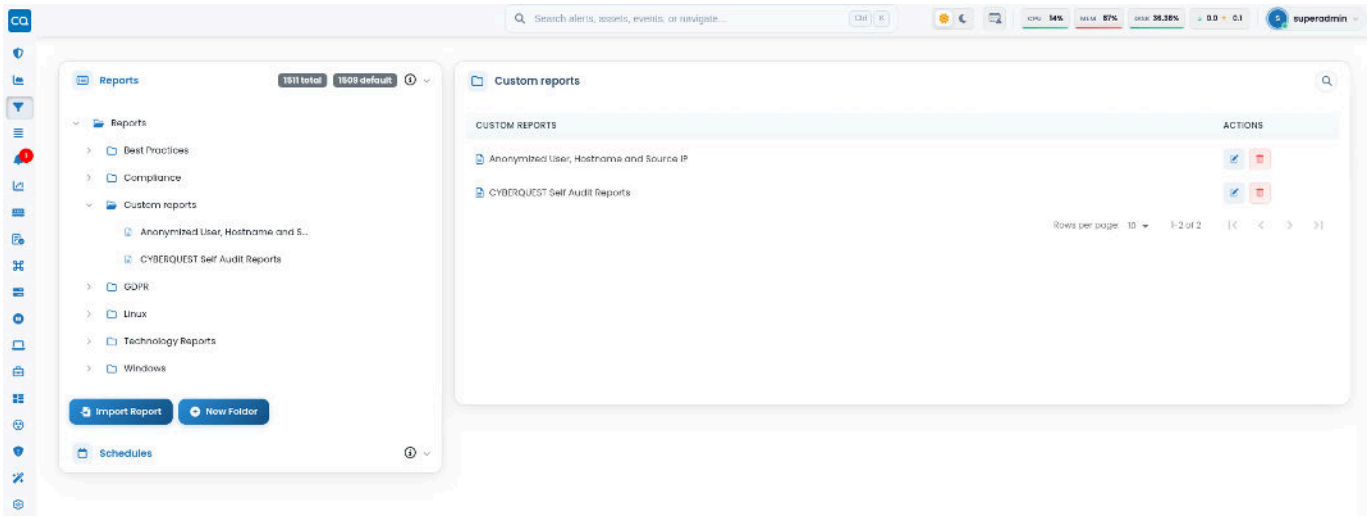


Save the report

Select the output fields to include, then click “**Save**”.



The report appears on the Reports page, under the Custom reports folder.



How to run a report

Navigate to the Reports page. The Custom reports folder contains user-created reports.

Navigate to Reports

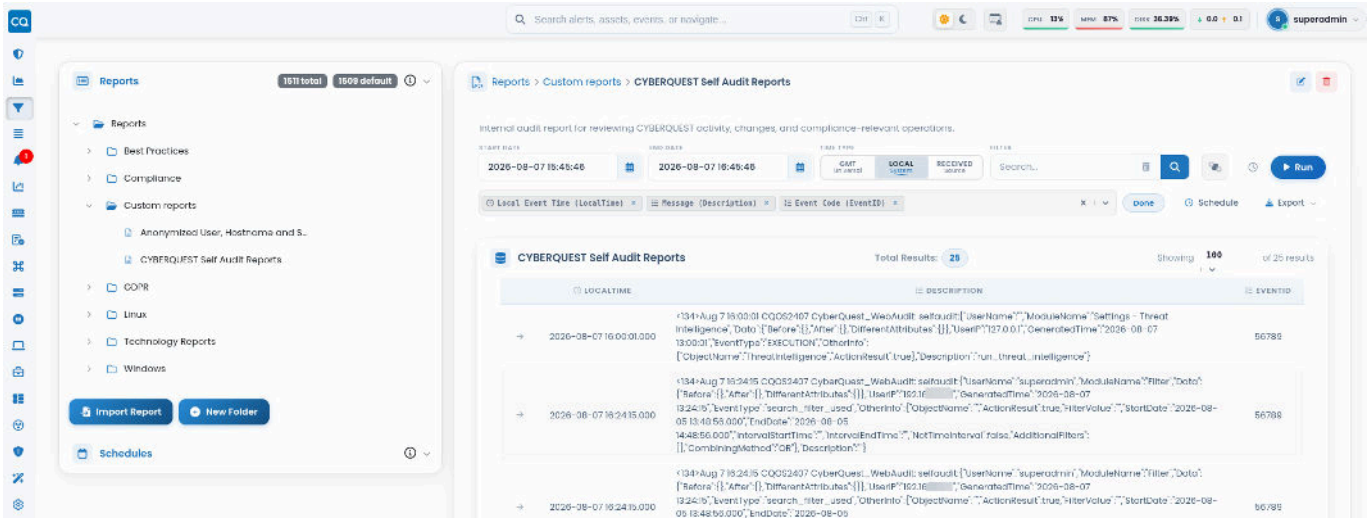
Open Reports and select a report (for example, Self Audit Reports).

Execute report

Choose a time interval and output fields, then click Execute Report.

Execution options control what data is included in the report:

- Set a specific **Start Date** and **End Date**
- Choose **Items on page** (100, 50, or 10)
- If **Time interval** is selected, pick the daily time window applied across the date range
- Adjust the time reference (local time, GMT, or event time) to shift displayed times accordingly
- Use **Filter Data** to include only matching entries (free-text search)
- Below **Filter Data**, select event fields to include in the report



Operations · How to create a parser

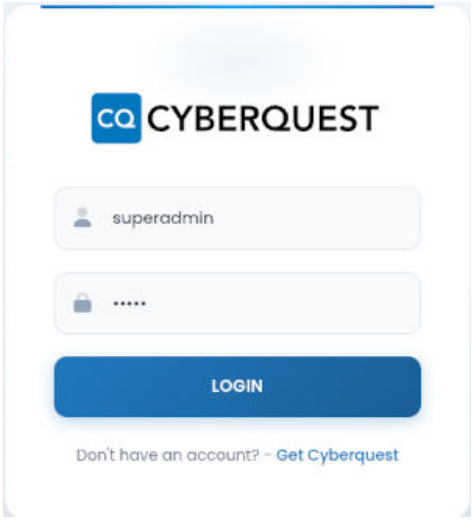
The JS parser object is available in user-customizable scripts within Data Transformation Service (DTS) and Alerts.

DTS is a JavaScript-based parsing service that provides various functions. Its primary role is to perform additional transformations on data extracted from collected events.

Authentication

To access the web interface, open a browser and enter the application's IP address or DNS name. The default address initially assigned to the web interface is ***https://CyberquestIPAddress*** (example).

The browser automatically redirects to CYBERQUEST's authentication page:



Navigate to Settings

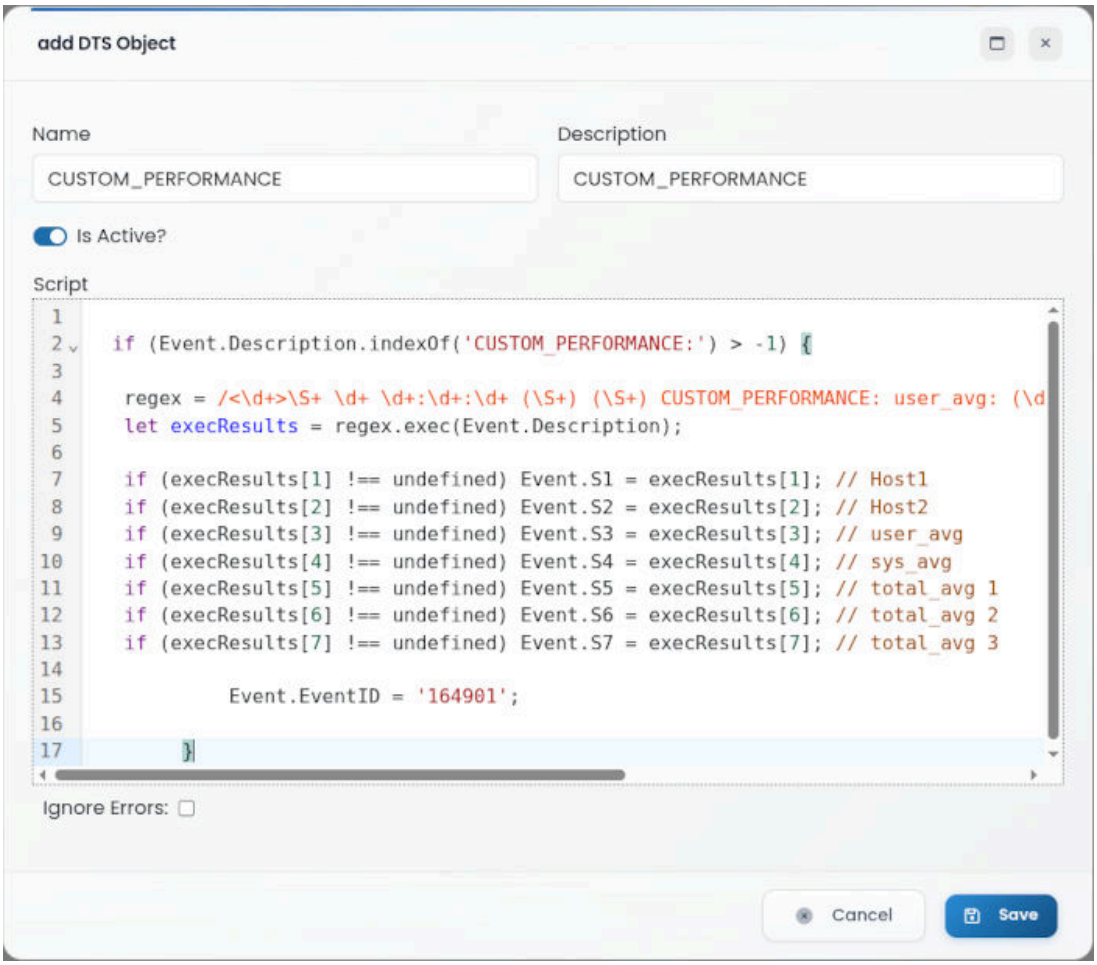
Navigate to **Settings > Rules** and select **DTS Objects**.

DTS Objects

Click **IMPORT OBJECT** to import a DTS object, or **ADD DTS OBJECT** to create a new one.



To create a new DTS object, click **ADD DTS OBJECT** and complete:



Name: A unique identifier for the DTS object.

Description: A brief summary of the object's purpose or functionality.

Is Active?: Determines if this object is enabled for execution.

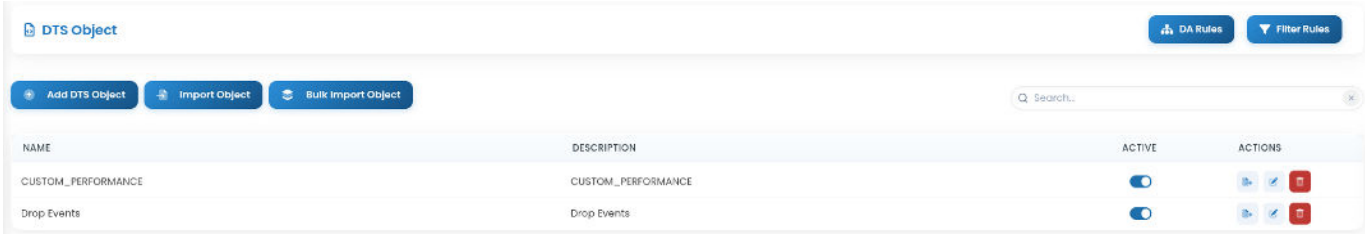
Script: The JavaScript code that runs within the DTS context to transform or process event data.

Ignore Errors: Determines whether the DTS should continue processing other objects if this script encounters an error.

Click **Save** to apply changes.

Actions menu

After creating the DTS object, the following actions are available:



- **Active/Inactive**:

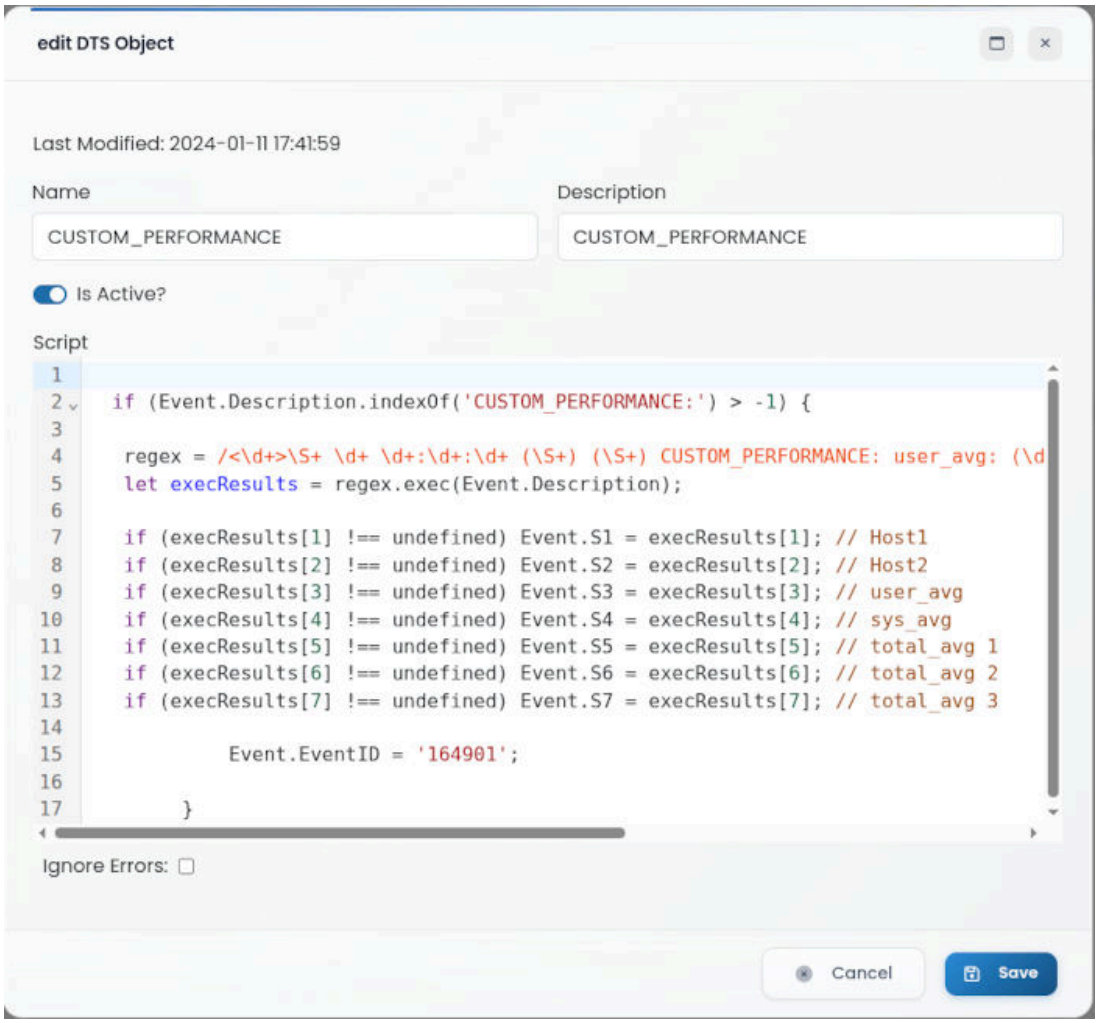
  Enable or disable the object with a single click.

- **Export**:

Export the object as a `.CQO` file for backup or transfer.

- **Edit**:

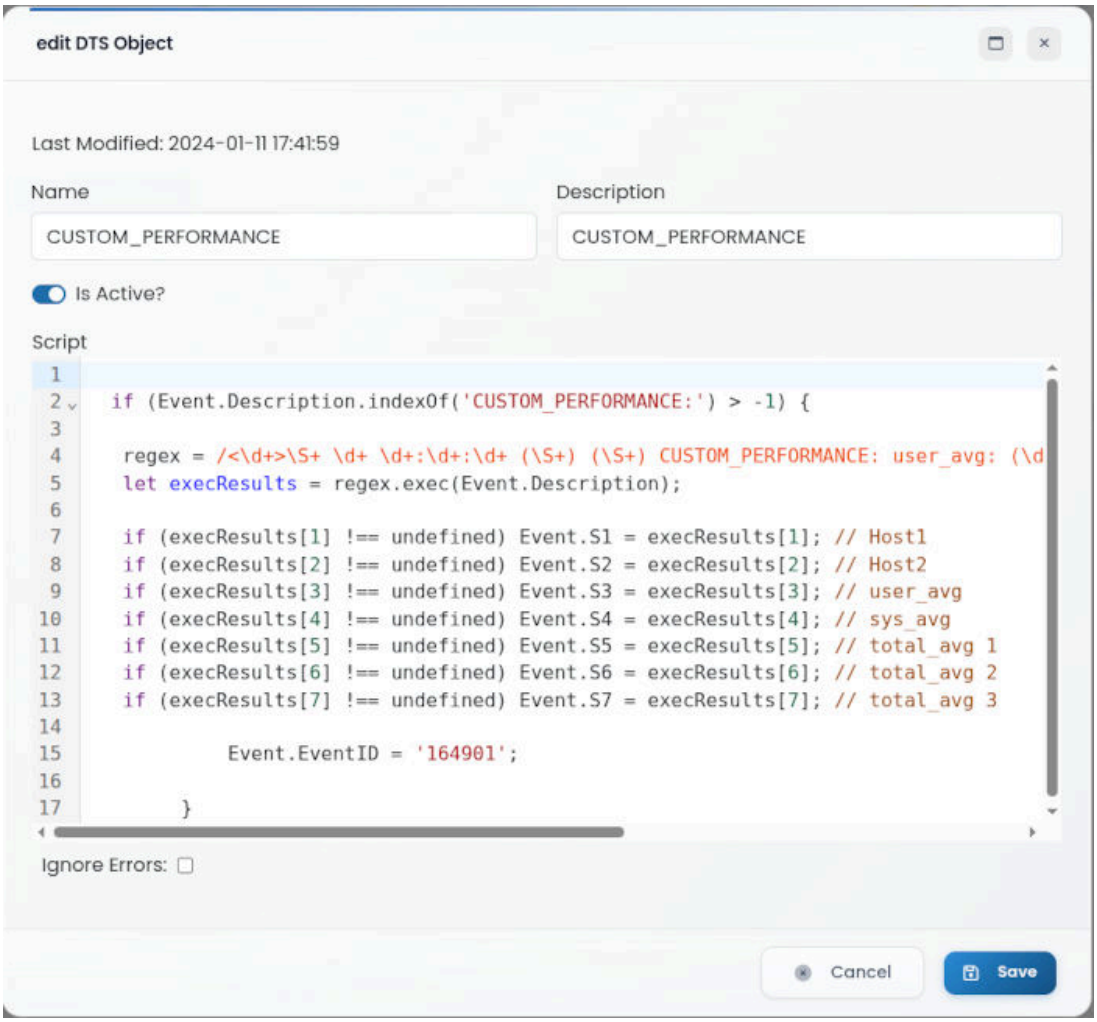
. Open the Edit page to modify the Name, Description, Script, or active/inactive state of the object.



- **Delete**: Remove the object permanently. Click Delete and confirm to proceed.

Example of parser

This example demonstrates enriching events by adding normalized fields derived from raw input data:



Operations · How to create a RTBF job

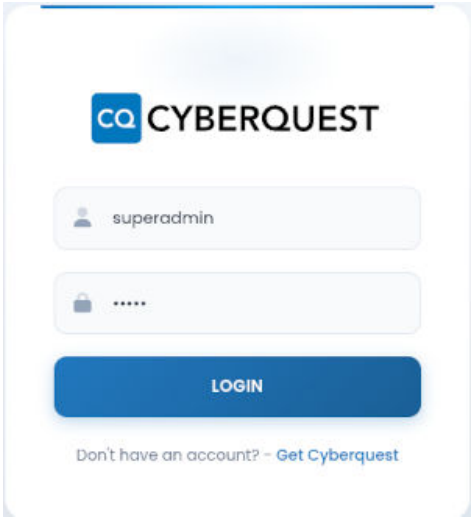
An RTBF (Right to be Forgotten) job deletes personal data based on matching patterns to support regulatory compliance.

To create this type of job, follow the steps described below:

Authentication

To access the web interface, open a browser and enter the application's IP address or DNS name. The default address initially assigned to the web interface is: ***https://CyberquestIPAddress*** (example).

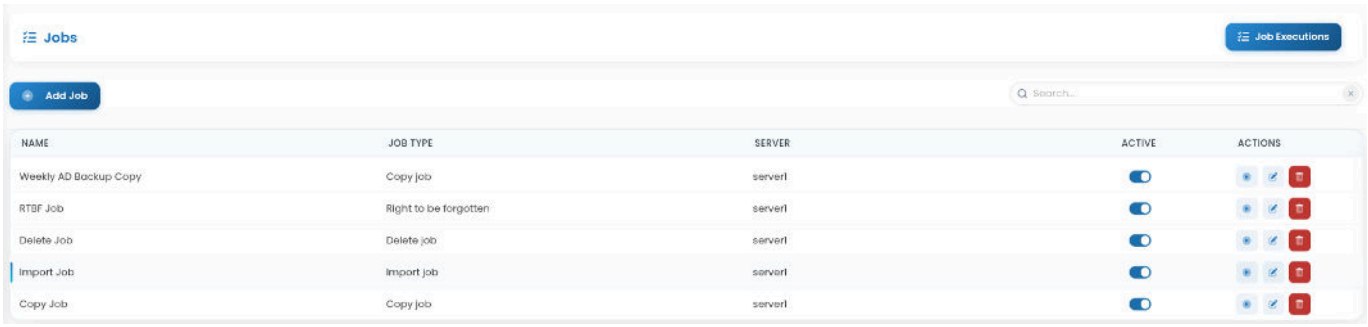
The browser automatically redirects to CYBERQUEST's authentication page:



Navigate to Settings

Navigate to **Settings > Jobs** and select **Jobs**.

This page contains all job types added in the CYBERQUEST application.



Edit Job: Click **Edit**



button to modify an existing job. The editing process is almost identical to adding a new job.

Start Job: Click **Start Job**



button to execute the job immediately. You can track its progress and status on the **Job**.

Delete Job: Click the **Delete** button



and confirm to permanently remove the job.

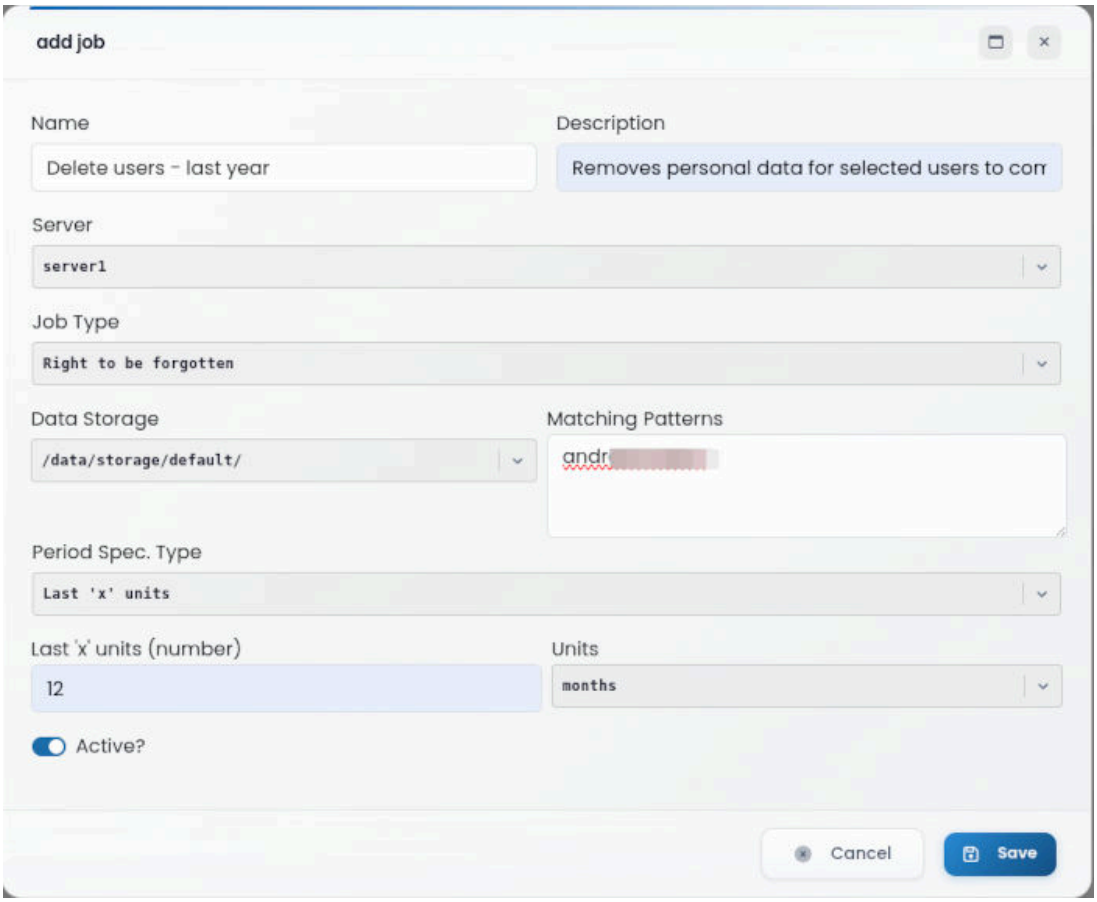
Active/Inactive: Use the toggle



to enable or disable the job without deleting it.

Create an RTBF job

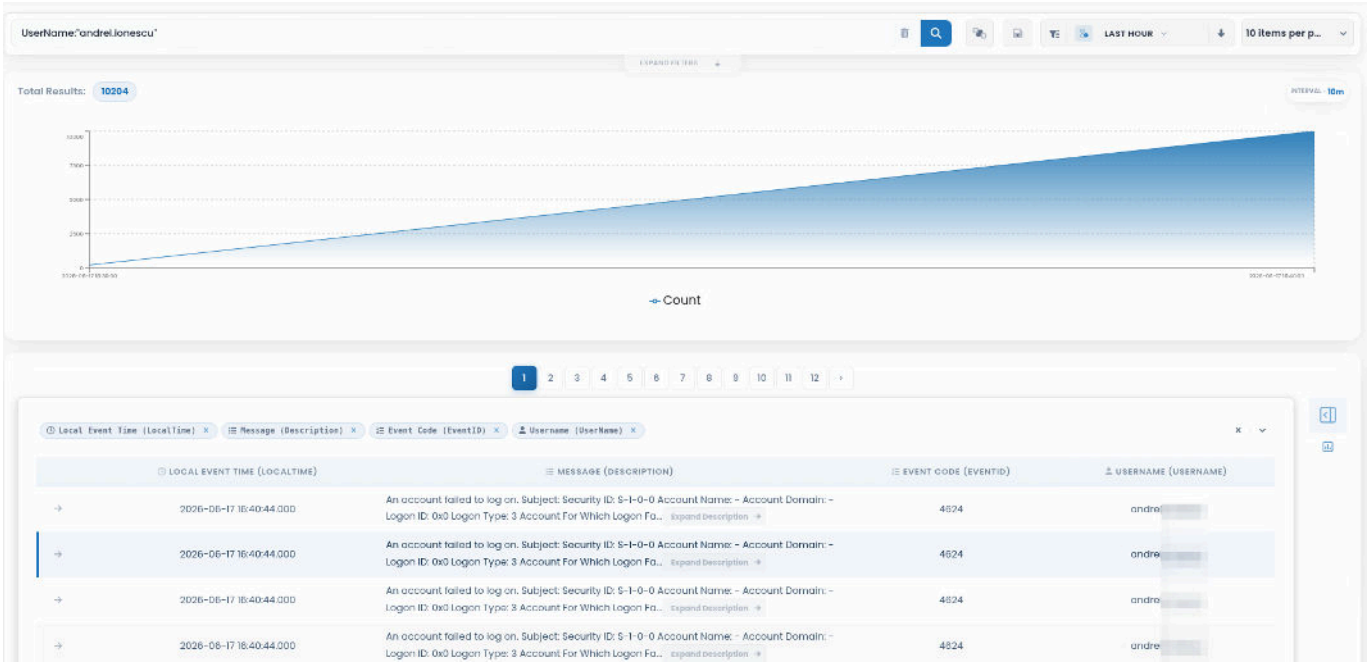
Click ***ADD JOB*** to create a new RTBF job. This opens the job configuration page where you can define the job's name, description, data source, matching patterns, filters, and schedule.



- **Name:** The display name of the job as it appears in the Jobs list.
- **Description:** A brief summary of the job's purpose or function.
- **Server:** The data server where the job will be executed.
- **Job Type:** Select the type of job to run.
  - **RTBF:** A job that deletes data based on defined filters or patterns to ensure regulatory compliance.
- **Data Storage:** The offline storage location that contains the data to be processed.
- **Matching Patterns:** Is used to search in data storage for all information matching the criteria.
- **Period Spec. Type:** Defines the time range of the data to be processed.
  - **Start Date / End Date:** Set a specific time window for data copying.
  - **Last 'x' units:** Define a rolling time frame (e.g., last 7 days).
- **Active:** Enables or disables the job.

When finished, click "Save" to apply changes or "Cancel" to discard.

Once the RTBF job has been created (prior to execution), events for the targeted user can be verified. Navigate to the **Browser** module, located on the left side of the interface. Apply the filter `UserName:"userFromMatchingPatterns"` and select the same time period defined in the RTBF job (*e.g., the last 12 months*) to confirm which events will be affected by the job.



Start Job: Click **Start Job**



button to execute the job.

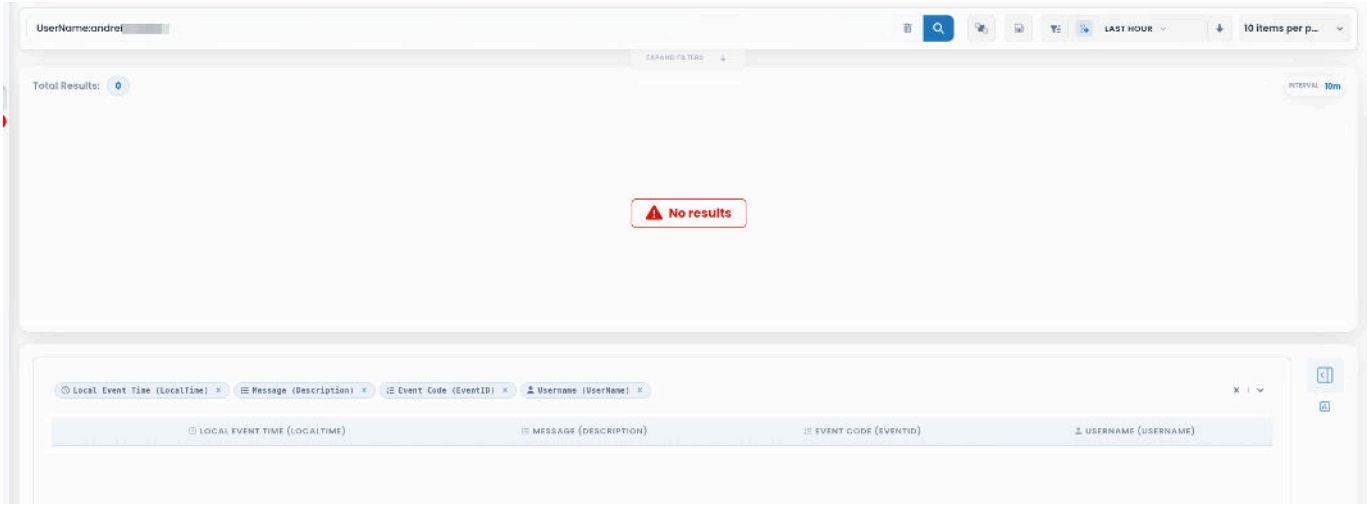


Verify the job execution

Open **Job Executions** from the **Jobs** page to confirm completion and review counts.



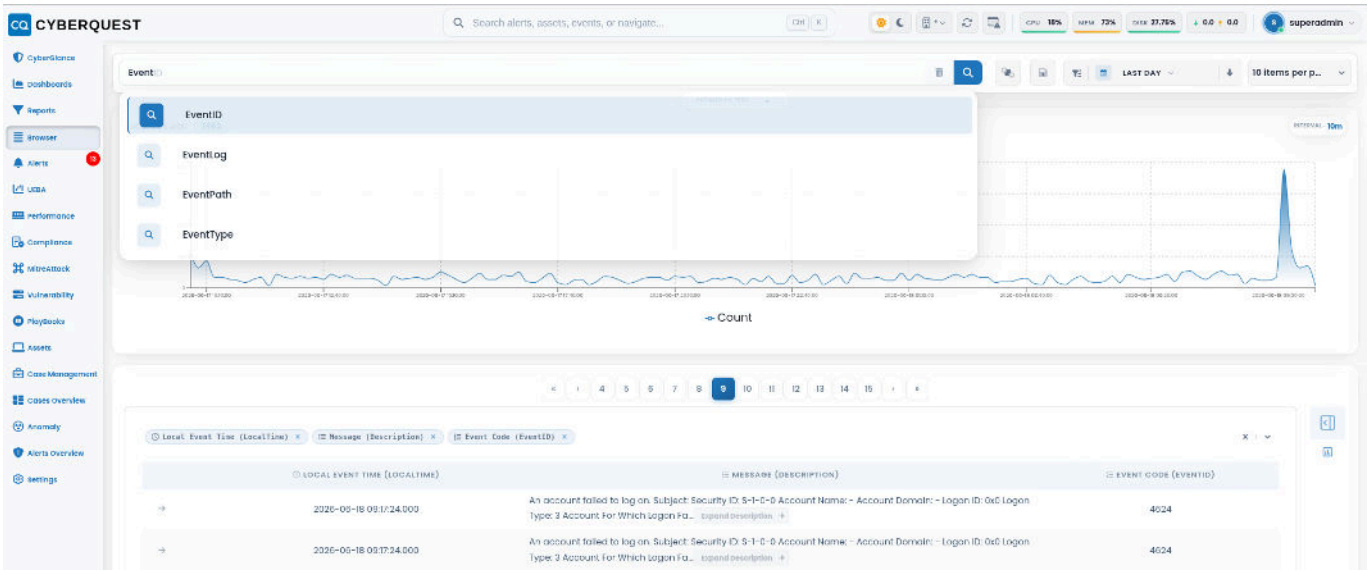
After the job has been executed, return to the **Browser** module and apply the same filter and time period to verify that the users events have been deleted. The absence of the events confirms that the RTBF job processed the data according to the specified criteria.



Operations · How to create an on-demand dashboard

Data filtering and ordering

For interactive investigations, filter, sort, and aggregate results directly within the interface. On-demand filter creation is supported, with field auto-completion for faster and more accurate queries.



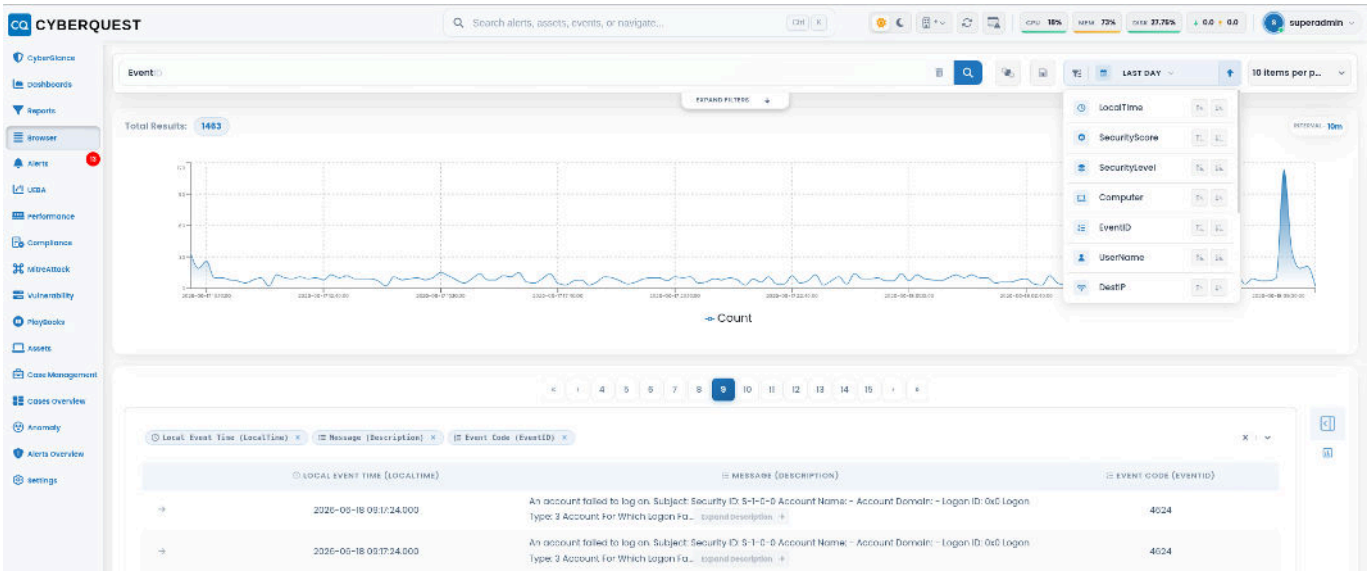
Once the filters are configured - either manually or by adding additional filters interactively via the GUI - data can be sorted by selected fields in ascending or descending order.

The options are:

Browser module:

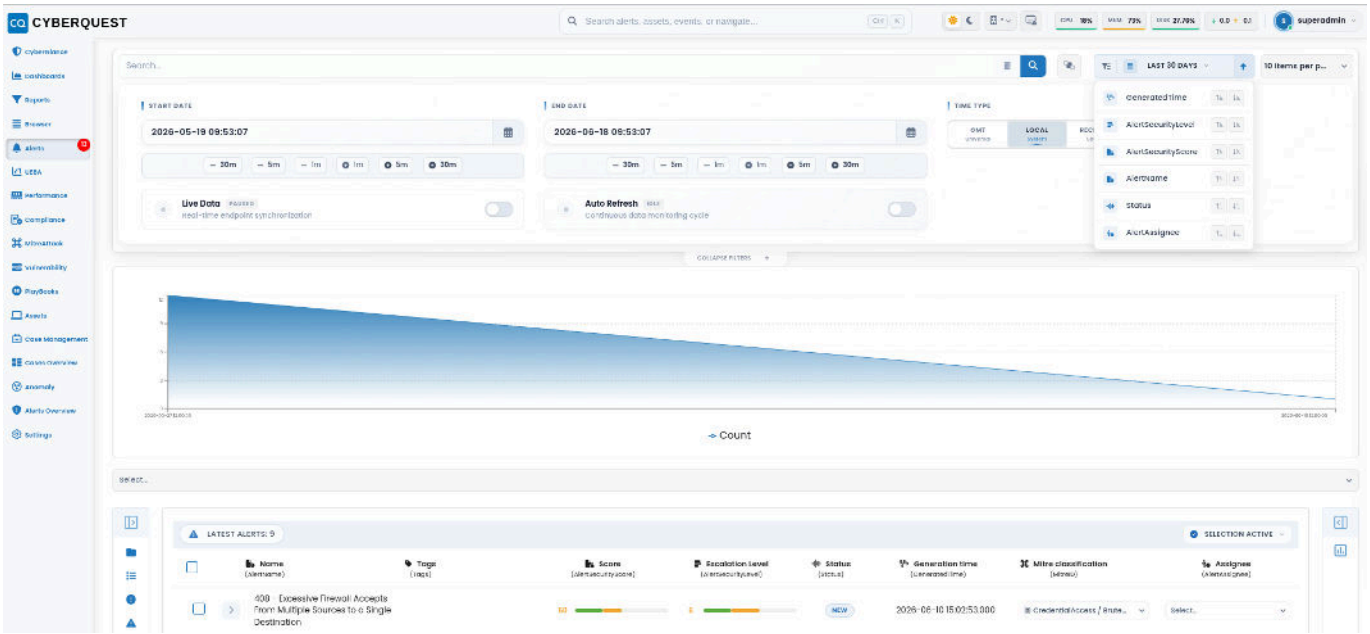
- `LocalTime` - The timestamp indicating when the event occurred on the local system. Useful for chronological sorting or identifying time-based patterns.
- `SecurityScore` - A numeric score representing the assessed security impact or severity of the event. Higher values typically indicate higher risk.
- `SecurityLevel` - A classification of the event's security importance (e.g., Low, Medium, High). Helps prioritize which events may require immediate attention.
- `Computer` - The hostname or identifier of the computer associated with the event. Useful for grouping or comparing events across multiple systems.
- `EventID` - A unique identifier assigned to the type of event, typically defining what action or condition triggered the log entry.

- `SrcIP` - The source IP address associated with the event, indicating the system or endpoint that initiated it.
- `EventLog` - The name or type of the event log where the entry was recorded (e.g., Application, System, Security).
- `Category` - A classification that indicates the event's type.
- `_event.Category` - A more specific or internal categorization imported directly from the underlying event data structure. Useful when the base *Category* field is too general.
- `RiskAssessment` - An evaluation of the potential threat level of the event, based on contextual analysis or predefined security criteria.



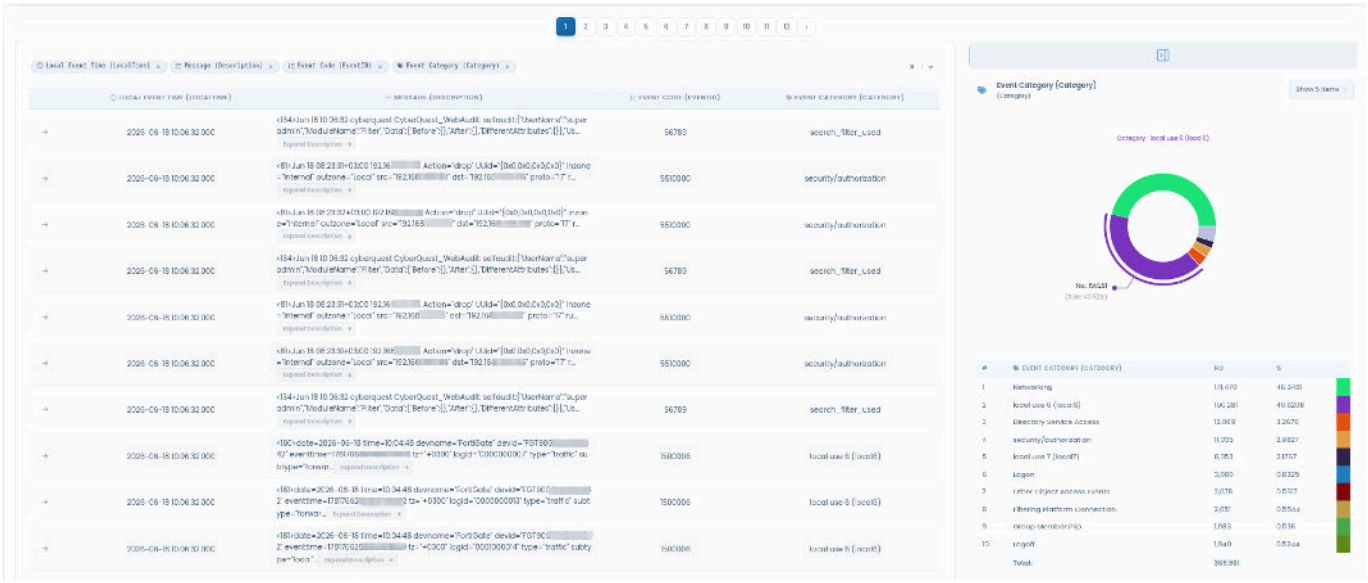
Alerts module:

- `GeneratedTime` - The timestamp when the alert was created. Useful for tracking when issues were first detected.
- `AlertSecurityScore` - A numeric score representing the severity or potential impact of the alert. Higher values indicate higher risk.
- `AlertSecurityLevel` - A classification of the alert's importance (e.g., Low, Medium, High). Helps prioritize which alerts require immediate attention.
- `AlertName` - The descriptive name of the alert, indicating the type of issue or event detected.
- `Status` - The current state of the alert, for example, New, Acknowledged, or False positive. Useful for monitoring workflow and follow-up actions.
- `AlertAssignee` - The person or team responsible for handling or investigating the alert. Useful for accountability and tracking resolution.



On-demand data aggregation

CYBERQUEST enables quick aggregation of the current results into a dashboard. Simply drag a column header onto the chart icon to create visual summaries instantly.

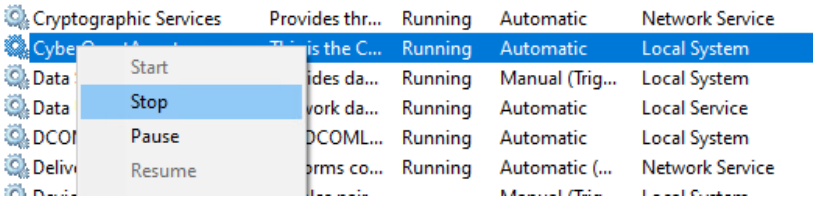


Operations · How to create Backups

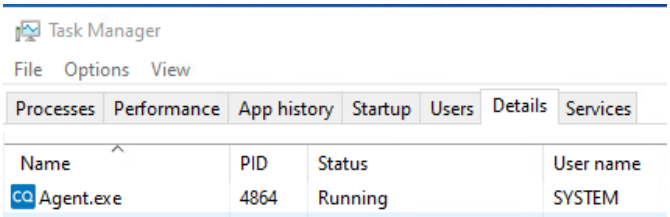
1.Backup CYBERQUEST Agent

In the event of a disaster, to save the Agent's configurations and data sources, please follow these steps:

A. On the Windows machine where the CYBERQUEST Agent is installed, open Windows Services and **stop** the CYBERQUEST Agent service.



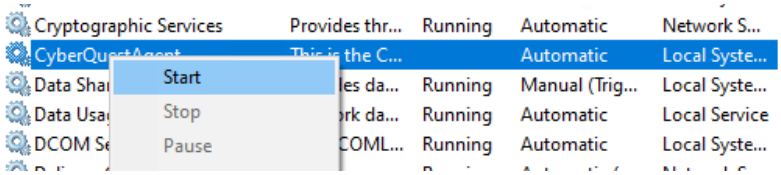
To check if the CYBERQUEST Agent has stopped, open **Task Manager > Details** and wait until the **Agent.exe** process disappears from Task Manager.



B. Copy the folder **datasources** to another machine. The folder is in the following path:

```
C:\Program Files\CyberQuestAgent\datasources
```

C. Open Windows Services and **start** the CYBERQUEST Agent service.



To verify that the CYBERQUEST Agent has started, open **Task Manager> Details** and wait until the **Agent.exe** process appears in the Task Manager.

2.Backing up configuration server side

To back up configurations, we need to export the two databases, config and reports.

Config contains CYBERQUEST application settings such as alert settings, jobs, dictionaries, and CYBERQUEST service settings.

Reports contains CYBERQUEST application customizations at dashboards, dashgroups, reports, agents and users.

To back up the two databases, we need to follow these steps:

A.Authenticate in CYBERQUEST server via ssh

B.Change the path using the following command:

```
cd /home/superadmin/
```

C.Create the folder **bkp** where the data will be saved:

```
mkdir  bkp
```

D.Change the path to the newly created folder:

```
cd bkp
```

E.Use the following commands to back up the two databases:

```
mysqldump -u root -p --databases reports > reports.sql
```

```
mysqldump -u root -p --databases config > config.sql
```

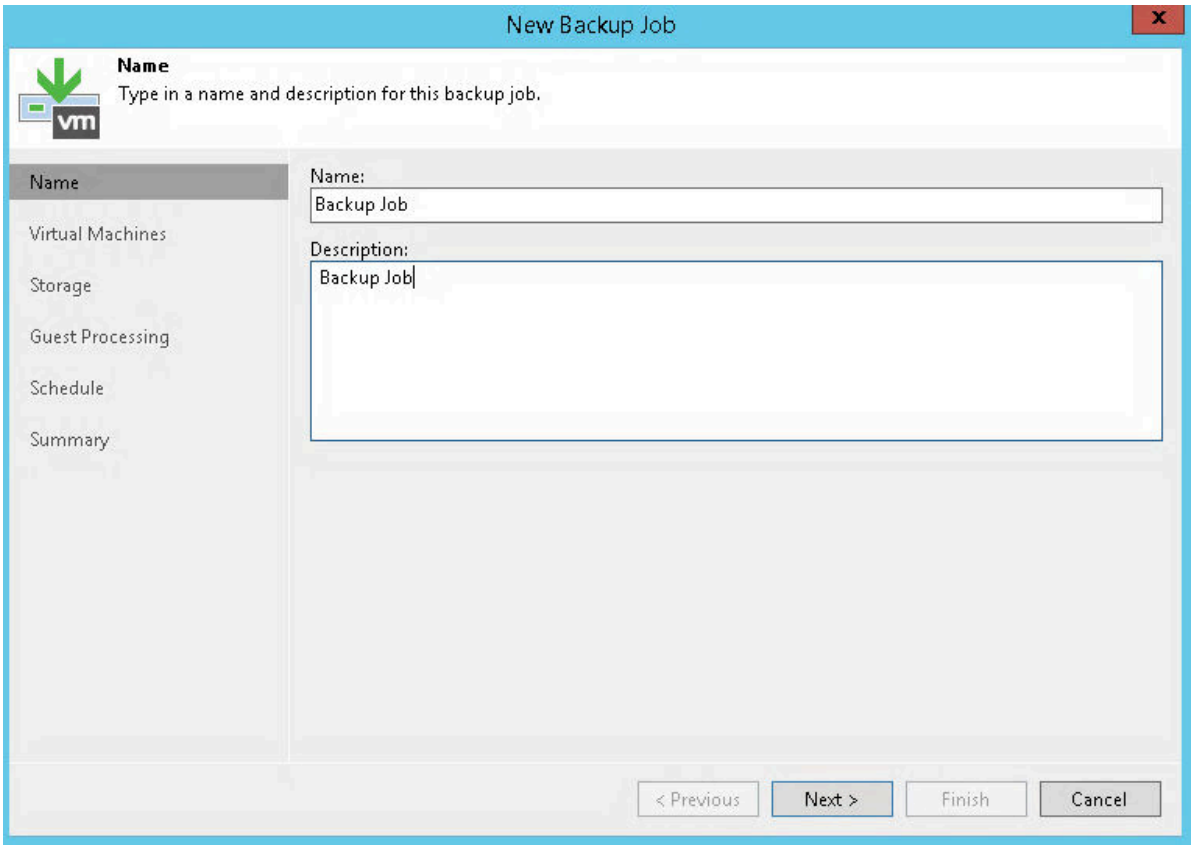
F.Copy the **bkp** folder to another machine to complete the backup process.

3.Backup Virtual Appliance

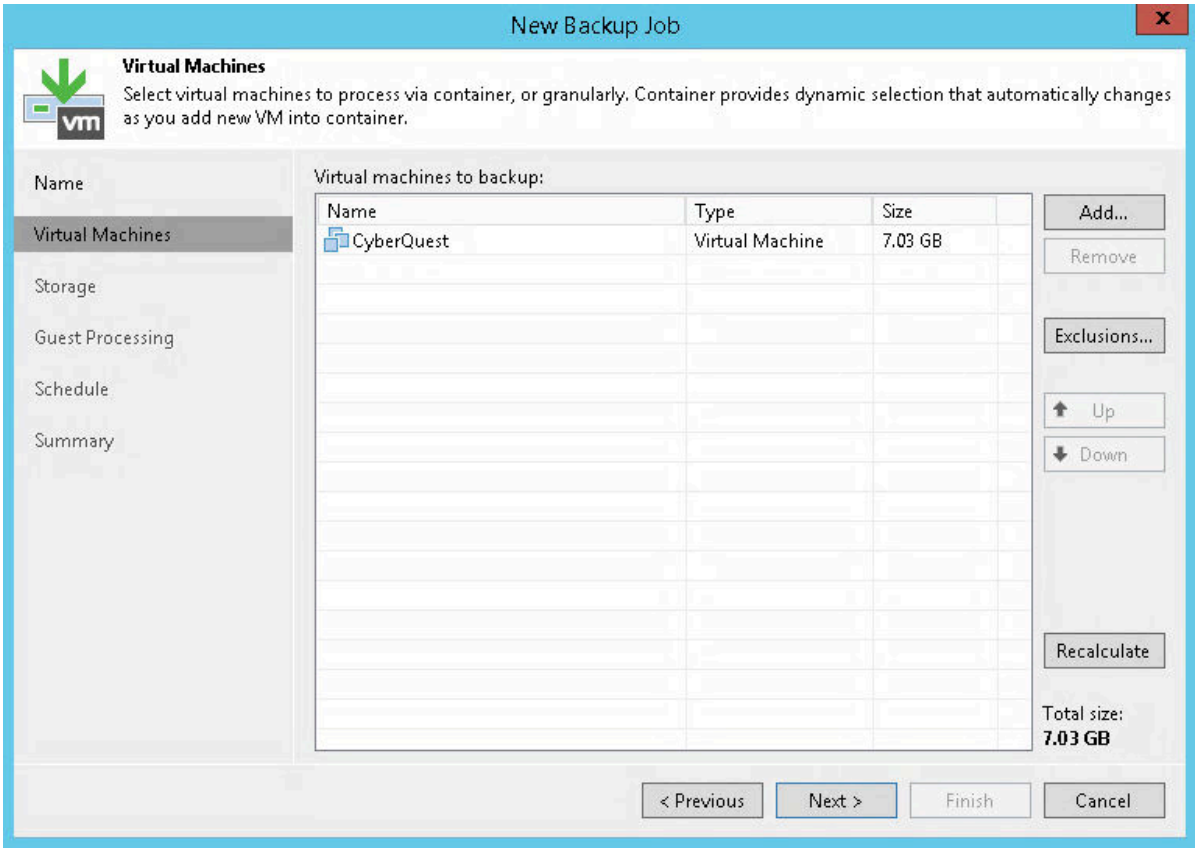
It is recommended to use a tool for backing up virtual appliances. Many tools on the market, like VEEAM or Quest Rapid Recovery, use an agent installed on hypervisor to handle virtual machines, therefore installing nothing on the virtual machine itself.

A.Open Veeam application

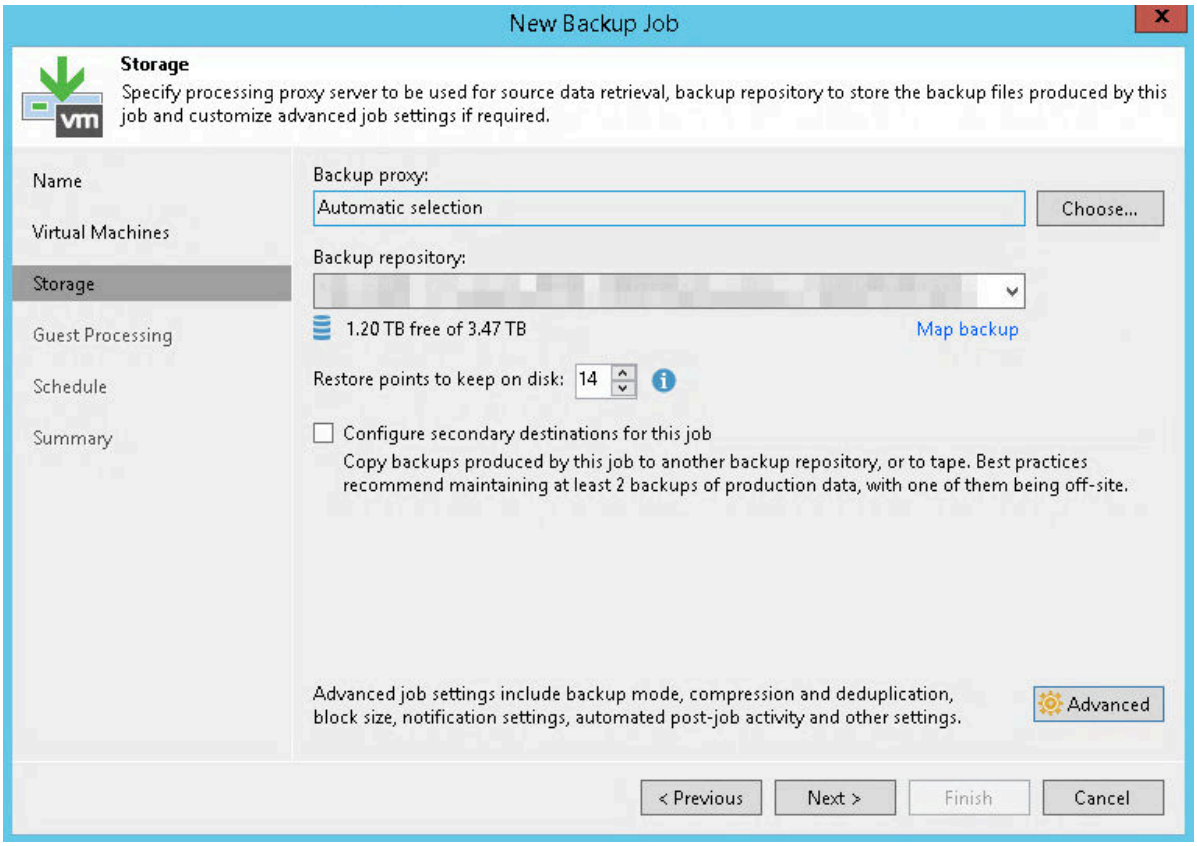
B.Create a Backup Job. Add name and description



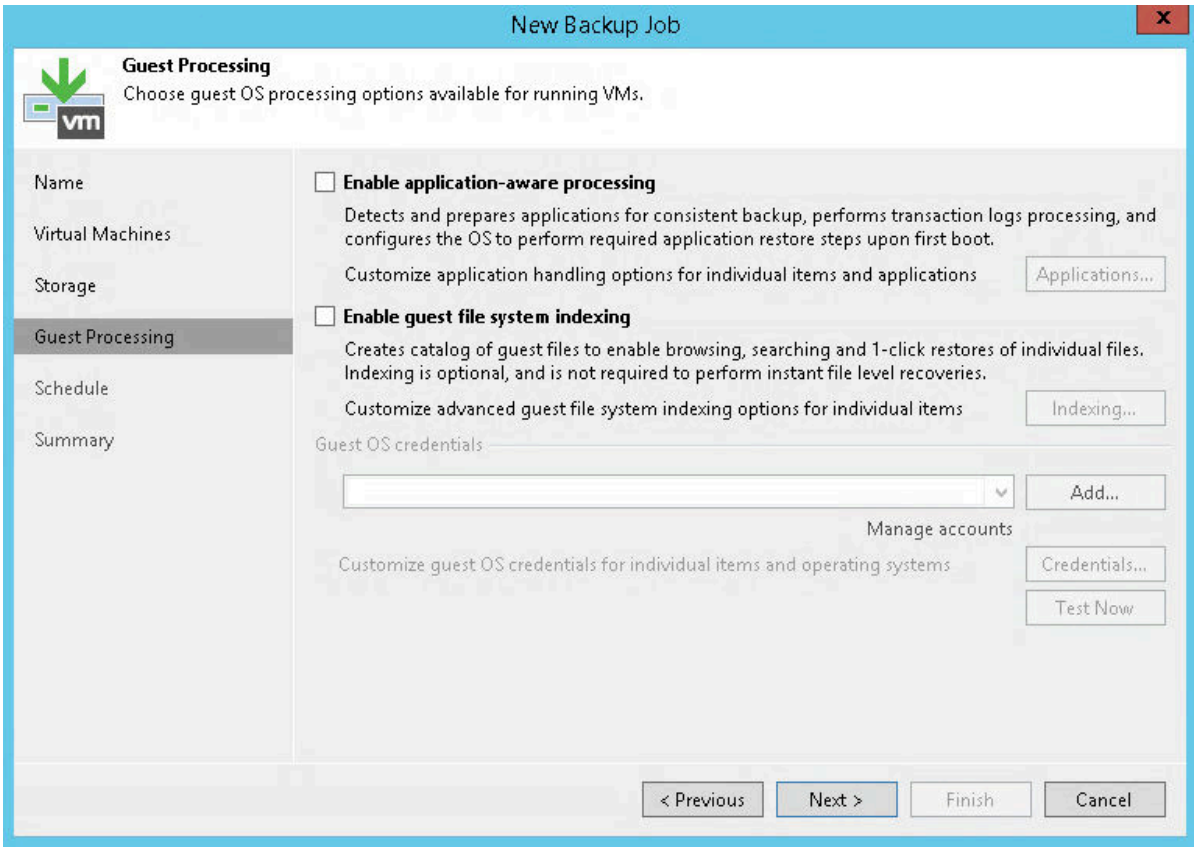
C.Select Virtual Machine to backup data



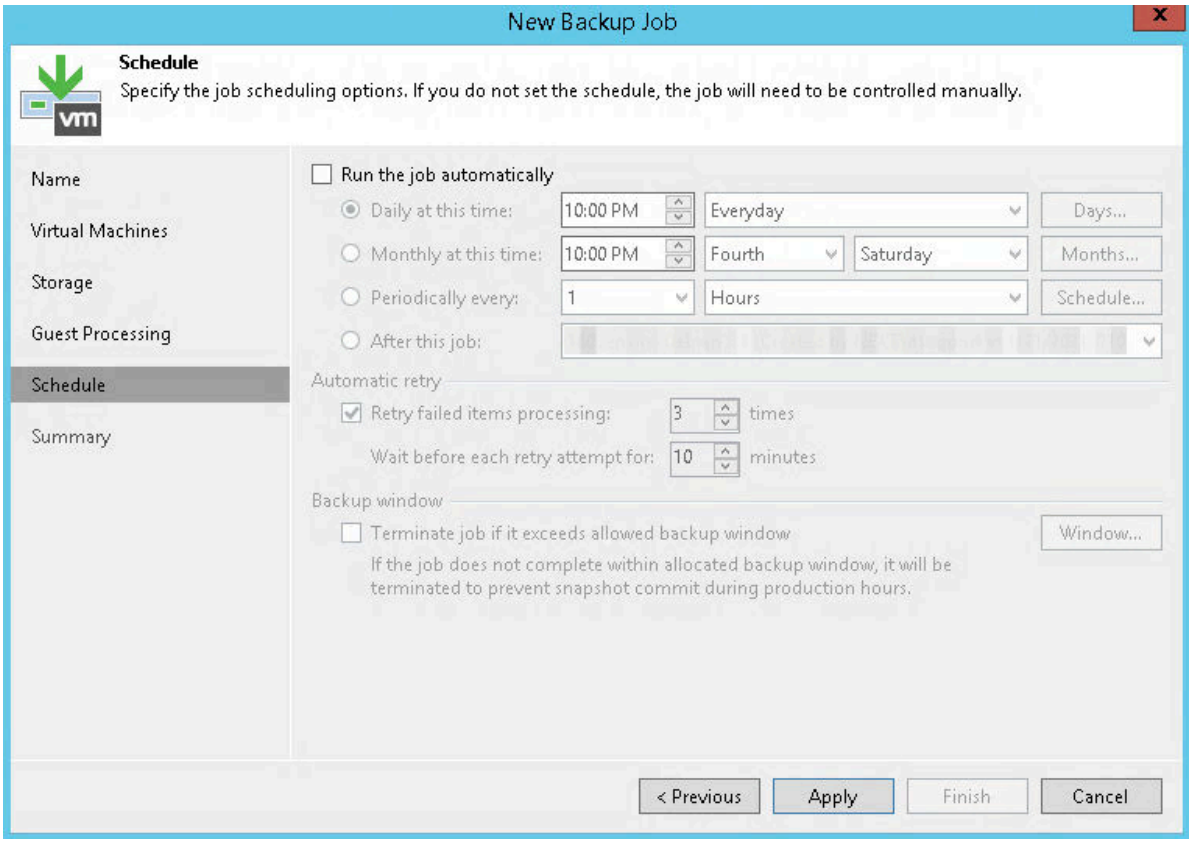
D.Select backup repository to save data and number of restore days



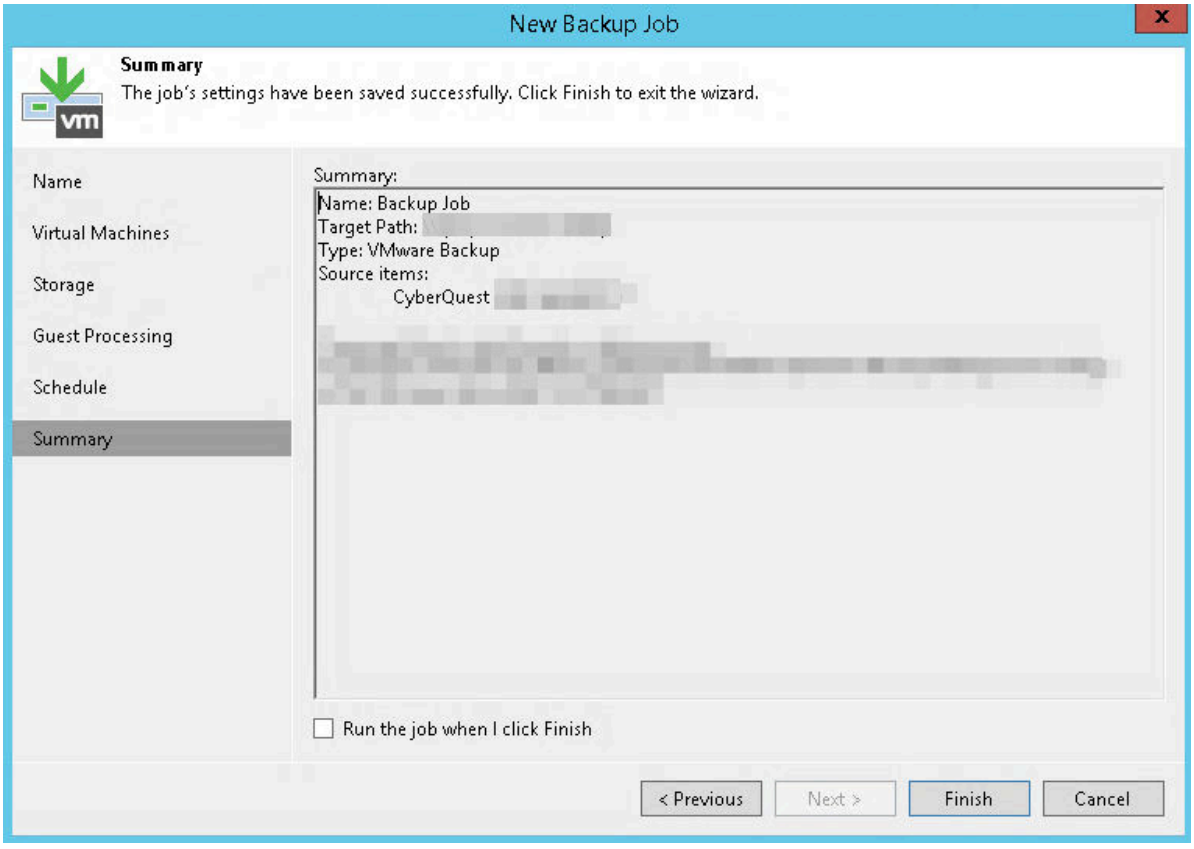
E.Choose guest OS processing options



E.Schedule the execution job

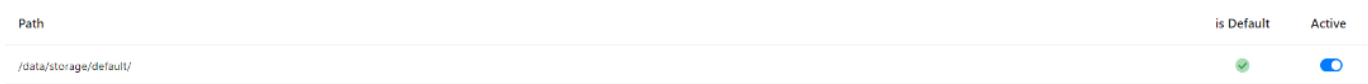


F. Summary



4.Backup data storage data

Every message collected by CYBERQUEST is automatically sent to data storages, as configured in **Settings > Data Storages** page:



Stored events are normalized in JSON format, compressed, encrypted and digitally signed. They can be later imported to a backup storage.

The default path is: **/data/storage/default**

The **default** folder must be copied to another external storage medium (outside CYBERQUEST).

5.Backup Online DataStorage data

Every message collected by CYBERQUEST is automatically sent to short term storage (Online DataStorage).

The default path is: **/data/elasticsearch**

The **Online DataStorage** folder must be copied to another external medium (outside CYBERQUEST).

Operations · How to delete data from Data Storage

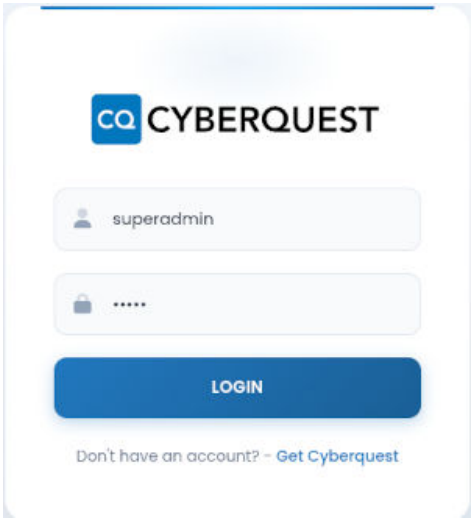
Create a *Delete job* to remove events from a data repository. This can be useful for freeing up storage space used by obsolete applications or cleaning up imported data.

Follow the steps below to create and configure this type of job:

Authentication

To access the web interface, open a browser and enter the application's IP address or DNS name. The default address initially assigned to the web interface is: ***https://CyberquestIPAddress*** (example).

The browser automatically redirects to CYBERQUEST's authentication page:



Navigate to Settings

Navigate to **Settings > Jobs** and select **Jobs**.

This page displays all job types that have been configured in the CYBERQUEST application.



Edit Job: Click **Edit**



button to modify an existing job. The editing process is almost identical to adding a new job.

Start Job: Click **Start Job**



button to execute the job immediately. You can track its progress and status on the **Job**.

Delete Job: Click the **Delete** button



and confirm to permanently remove the job.

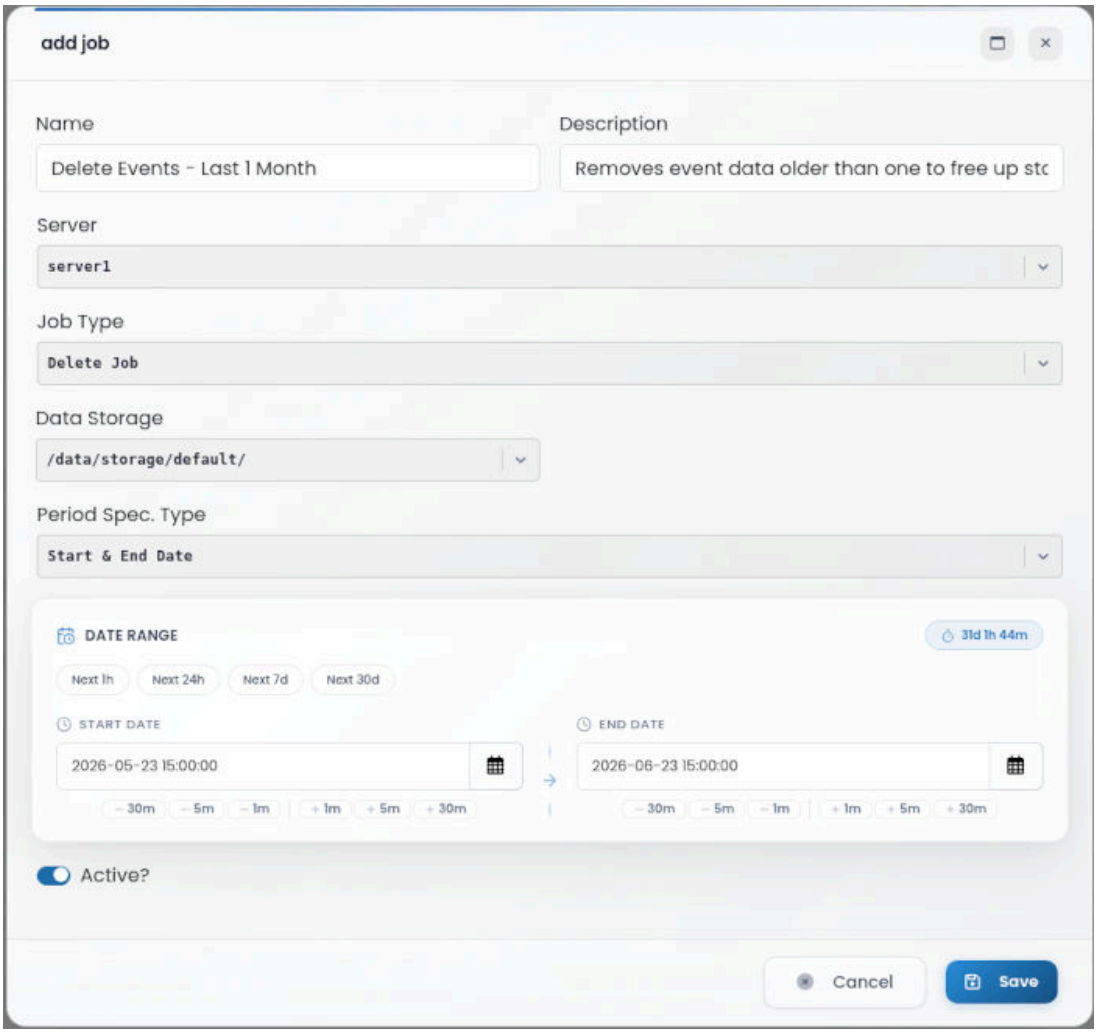
Active/Inactive: Use the toggle



to enable or disable the job without deleting it.

Create a delete job

Click ***ADD JOB*** to open the configuration page for creating a new delete job.



- **Name:** The display name of the job as it appears in the Jobs list.
- **Description:** A brief summary of the job's purpose or function.
- **Server:** The data server where the job will be executed.
- **Job Type:** Select the type of job to run.
  - **Delete Job:** A job that removes events from a repository based on the specified time period, helping to free up storage or clean up outdated data.
- **Data Storage:** The offline storage location that contains the data to be processed.
- **Matching Patterns:** Is used to search in data storage for all information matching the criteria.
- **Period Spec. Type:** Defines the time range of the data to be processed.
  - **Start Date / End Date:** Set a specific time window for data copying.
  - **Last 'x' units:** Define a rolling time frame (e.g., last 1 months).
- **Active:** Enables or disables the job.

When finished, click "Save" to apply changes or "Cancel" to discard.

Start Job: Click **Start Job**

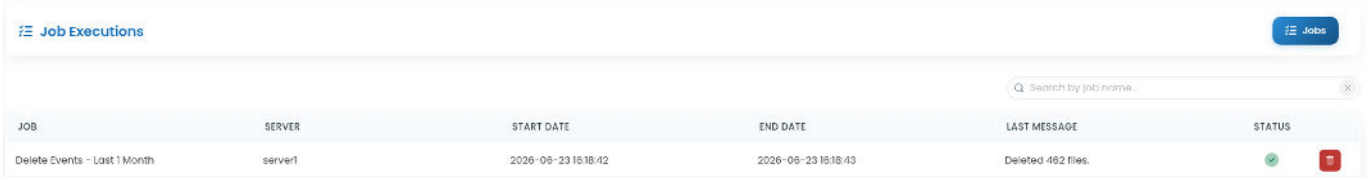


button to execute the job.



Verify the job execution

Open **Job Executions** from the **Jobs** page to confirm completion and review counts.



Operations · How to delete events older than 6 months

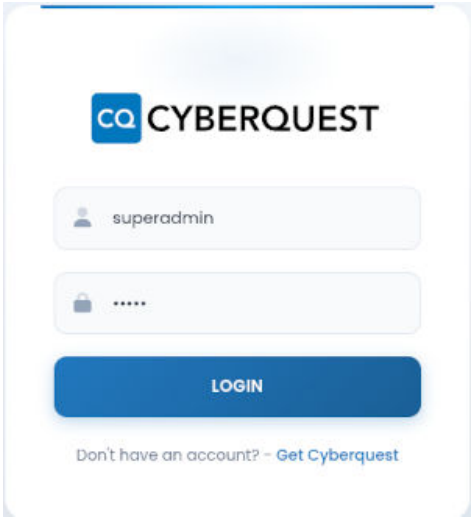
Set a retention policy and remove events older than the defined period from both archive (offline) and online stores.

All data is stored in two locations: the archive (offline) database and the online database. To delete events older than the required retention period, complete the two steps below.

A. Delete from archive (offline) database

Authentication

To access the web interface, open a browser and enter the application's IP address or DNS name (for example, ***https://CyberquestIPAddress***). The browser automatically redirects to CYBERQUEST's authentication page:

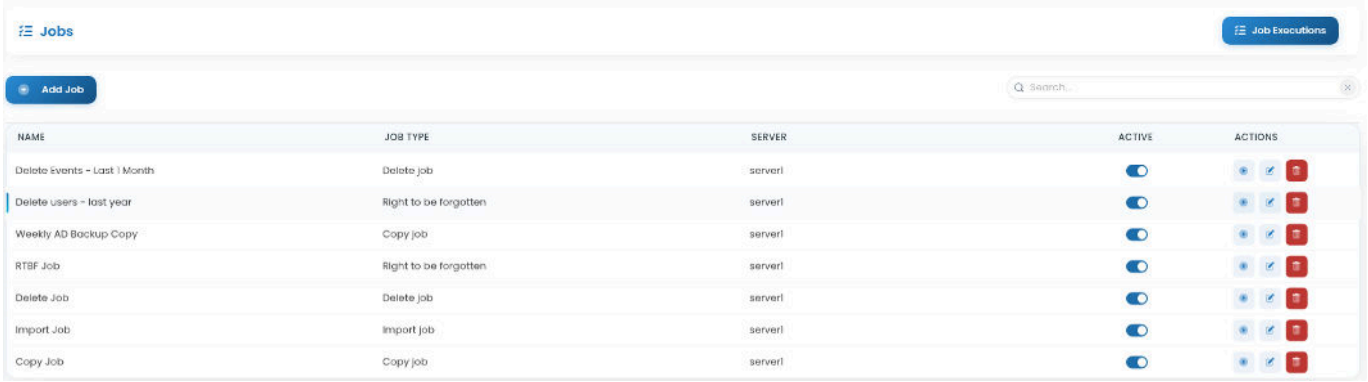


Navigate to Jobs

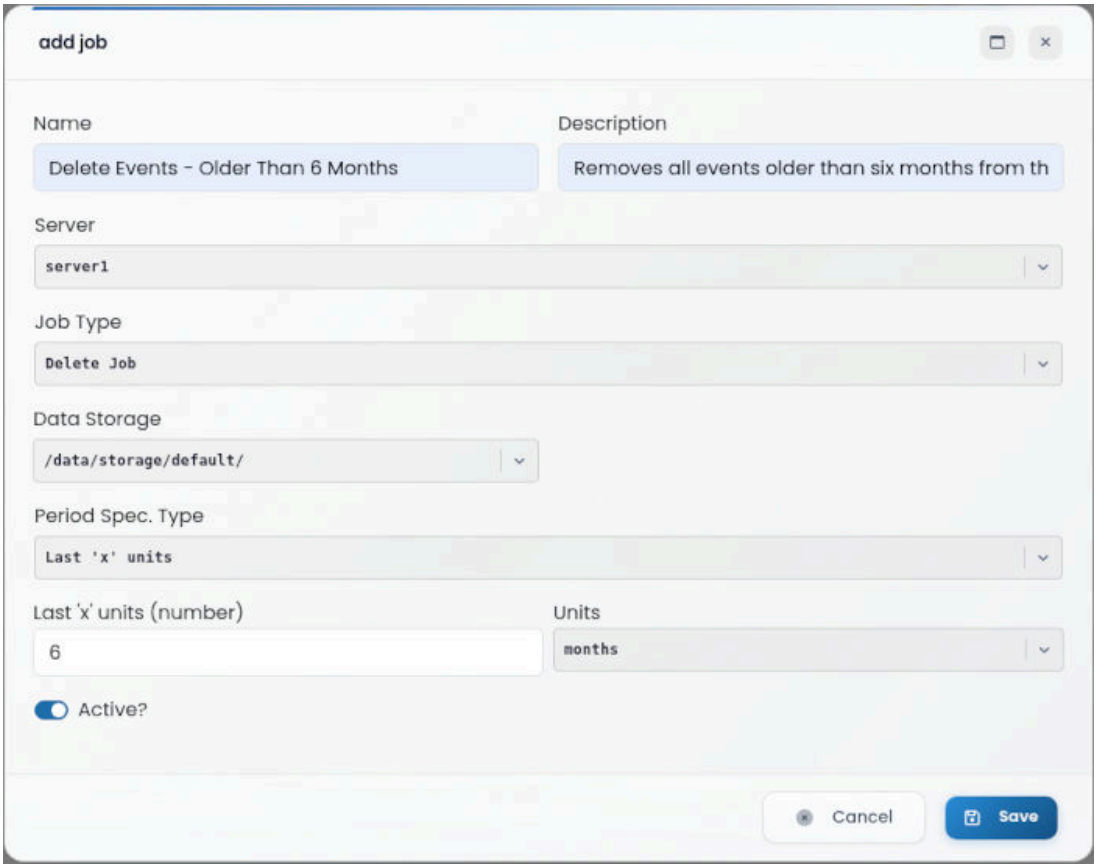
Navigate to **Settings > Jobs** and select **Jobs**.

Create a new job

Click the **Add Job** button in the top-left corner of the interface.



Complete the form to configure the job.



Name: Enter a descriptive name to identify the job in the Jobs list, for example: `Delete Events - Older Than 6 Months`

Description: Provide a short purpose, for example: `Removes all events older than six months from the offline repository to free up storage`

Server: Select the data server that manages the repository where the events are stored

Job Type: Choose **Delete job**

- **Delete Job:** Removes events from the specified repository based on the defined time window.

Data Storage: Select the offline data storage containing the events to delete.

Period Spec. Type: Choose **Last 'x' units** and set it to **6 months**. This ensures that only events older than six months are targeted by the job

Active: Mark the job **Active** to run immediately, or leave it inactive to schedule it for later execution.

Click **Save** to apply the configuration and create the job.

Execute the job

Execute the Job: Click **Start** to begin executing the job. The system will process the specified data according to the configured settings.



Job Executions

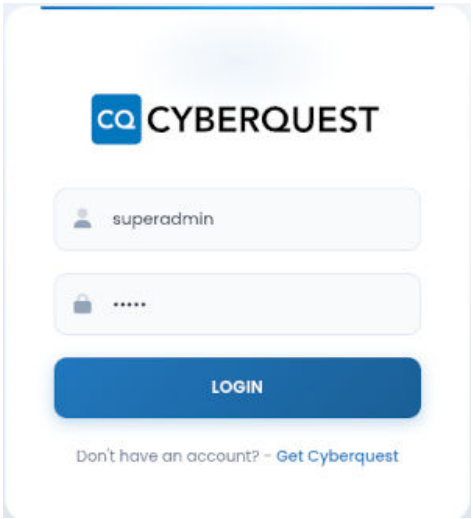
On the **Jobs** page (top-right), click **Job Executions** to monitor the status of jobs.



B. Delete from online database

Authentication

Log in to the web interface with an account with administrative rights.



Navigate to Retention Period

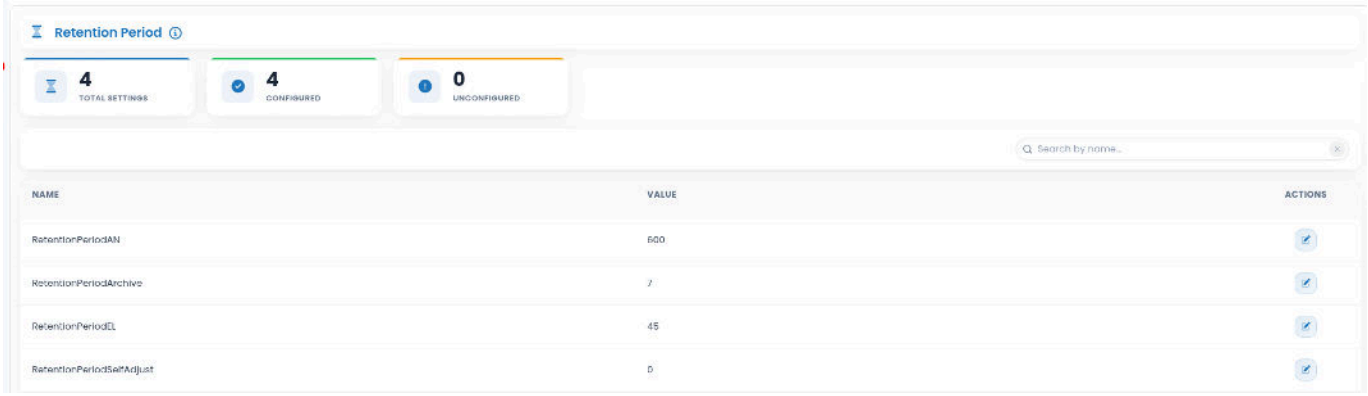
Navigate to **Settings > Application Settings** and select **RetentionPeriod**.

Edit Retention Period

To modify the **RetentionPeriodEL** settings, click the



button and update the value according to GDPR requirements or the organization's internal policies. Select the retention period and click **Save** to apply.



Operations · How to disable two-factor authentication (2FA) for a user account

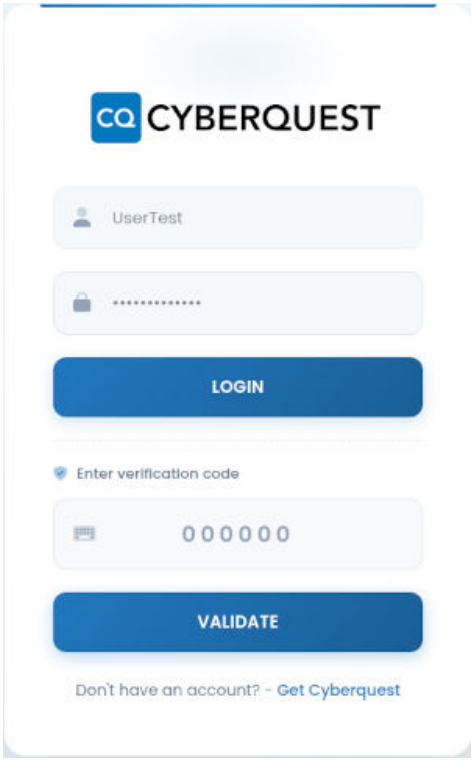
Two options are available:

- Disable 2FA as the user
- Disable 2FA as an administrator

1. Disable 2FA as the user

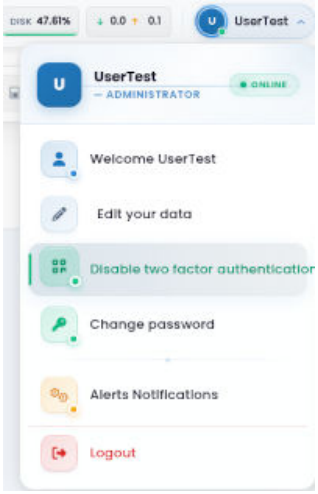
Log in with 2FA

- Access the CYBERQUEST web interface using a valid username and password.
- Enter the Google Authenticator code and click **Validate** to complete authentication.



Disable 2FA

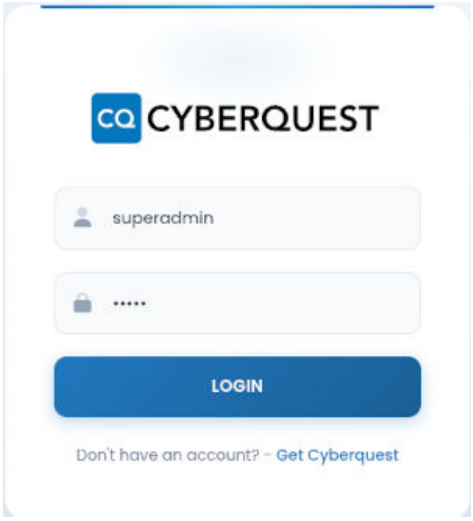
From the **Settings** menu, select **Disable two-factor authentication**. After disabling 2FA, the session ends and you are logged out.



2. Disable 2FA as an administrator

Authentication

Use an Administrator account to access the CYBERQUEST web interface (for example, ***https://CyberquestIPAddress***).



Navigate to Settings

From **Settings**, select **Users and groups > Users** to open the Users page.

Disable 2FA for a user

On the **Users** page, locate the target user and select the



action to disable two-factor authentication:



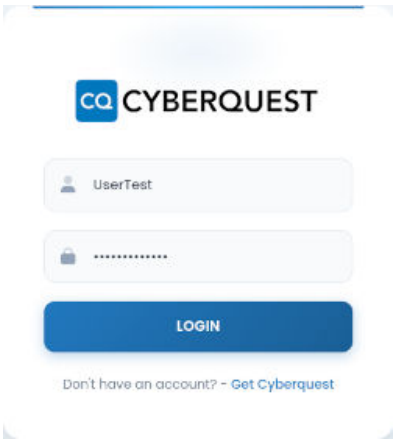
Operations · How to enable two-factor authentication (2FA) for a user account

With two-factor authentication (2FA), an additional layer of security is added to the account. In addition to the password, a time-based code generated by Google Authenticator on a mobile device is required. Follow the steps below to activate 2FA.

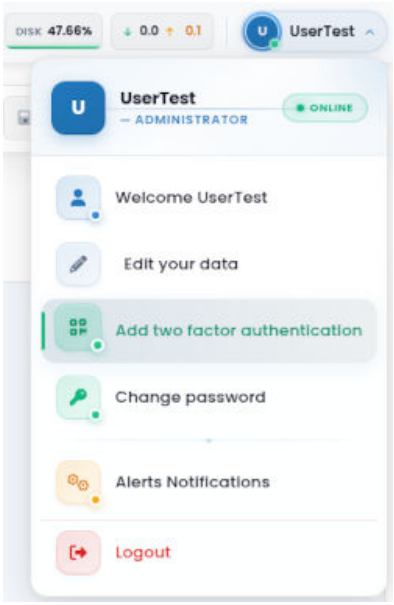
Authentication

To access the web interface, open a browser and enter the application's IP address or DNS name (for example, ***https://CyberquestIPAddress***). The browser redirects to the CYBERQUEST authentication page:

–

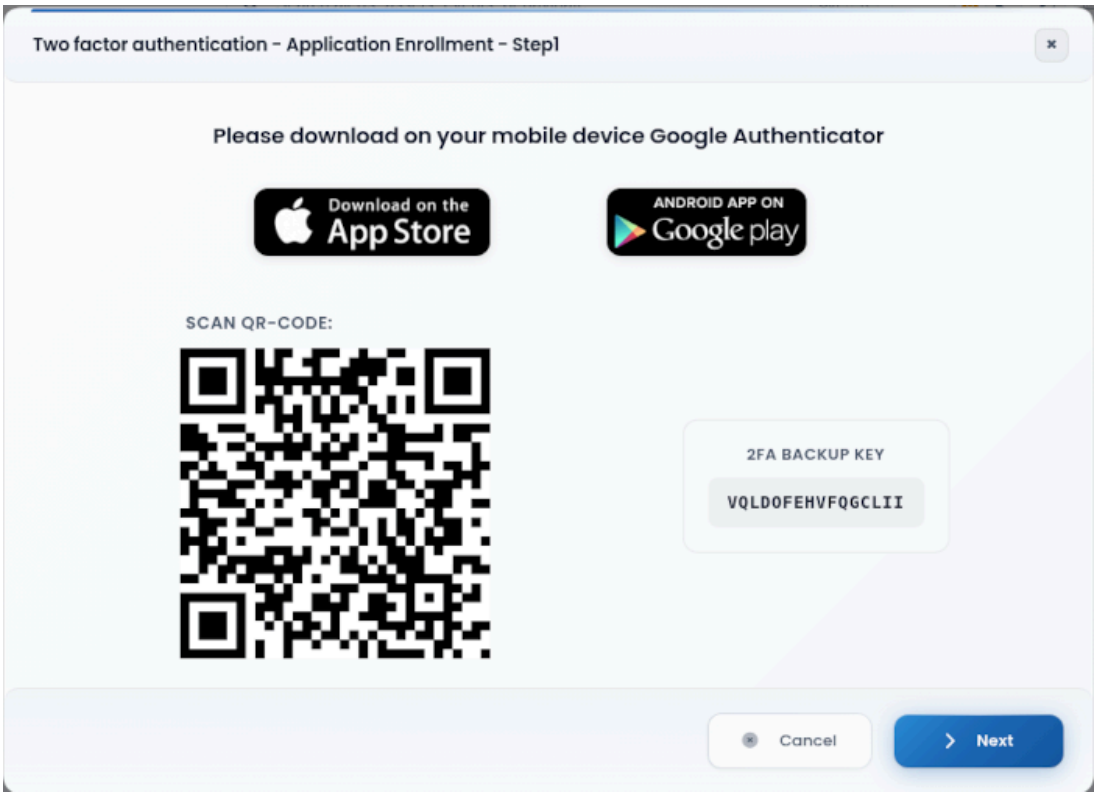


From the **User Enable Area**, click **Add Two-Factor Authentication** to open the configuration page.



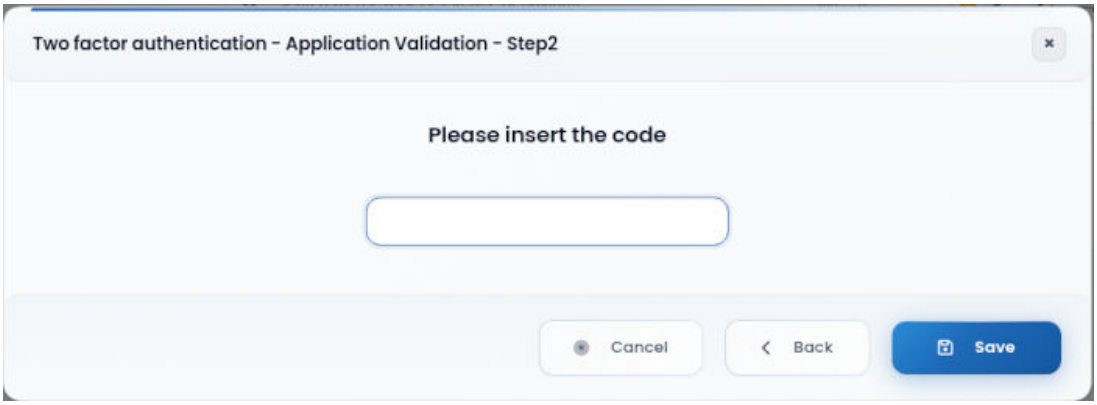
Application Enrollment

Scan the QR code or manually enter the backup key into Google Authenticator, then click **Next**.



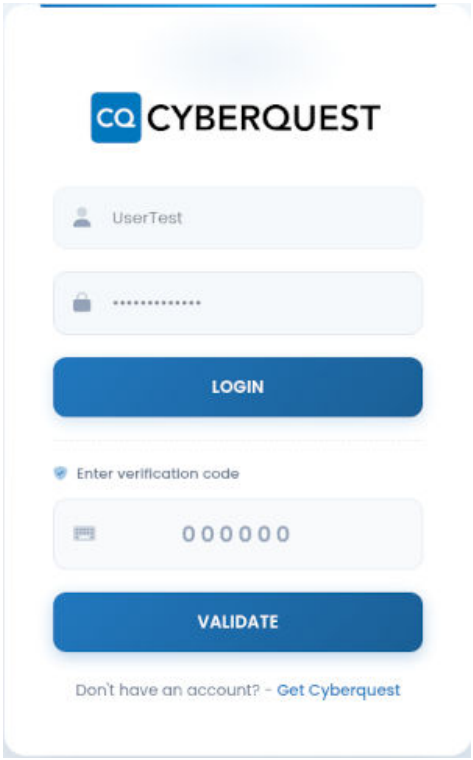
Application Validation

Enter the code generated by Google Authenticator and click **Save** to complete the setup.



Verification

Sign in using the username and password, then enter the two-factor authentication (2FA) code and click **Validate**.

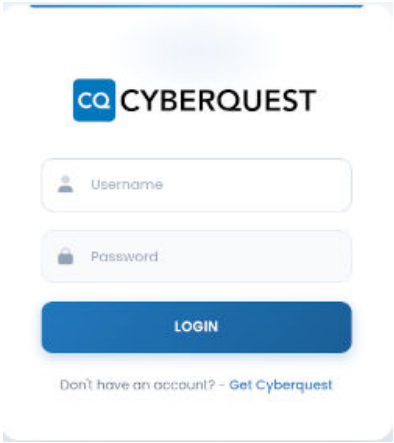


Operations · How to export data from dashgroup

Export a graphical report (PDF) based on aggregated events or alerts from any dashgroup.

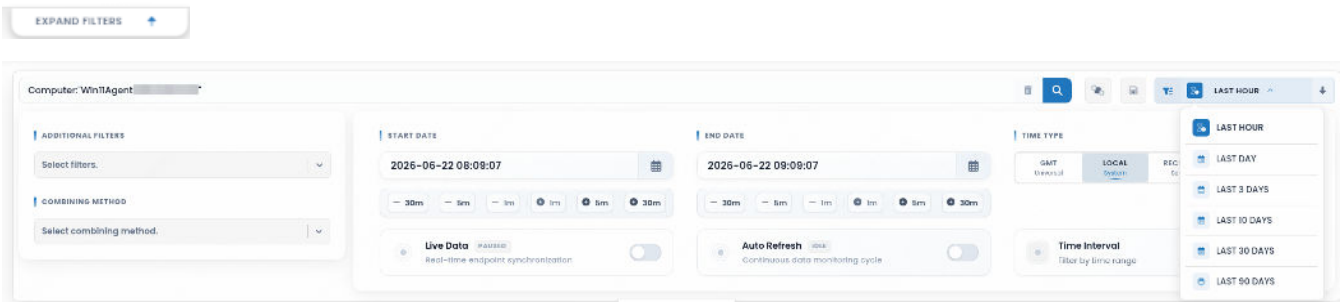
Authentication

To access the web interface, open a browser and enter the application's IP address or DNS name (for example, ***https://CyberquestIPAddress***). The browser redirects to the CYBERQUEST authentication page.



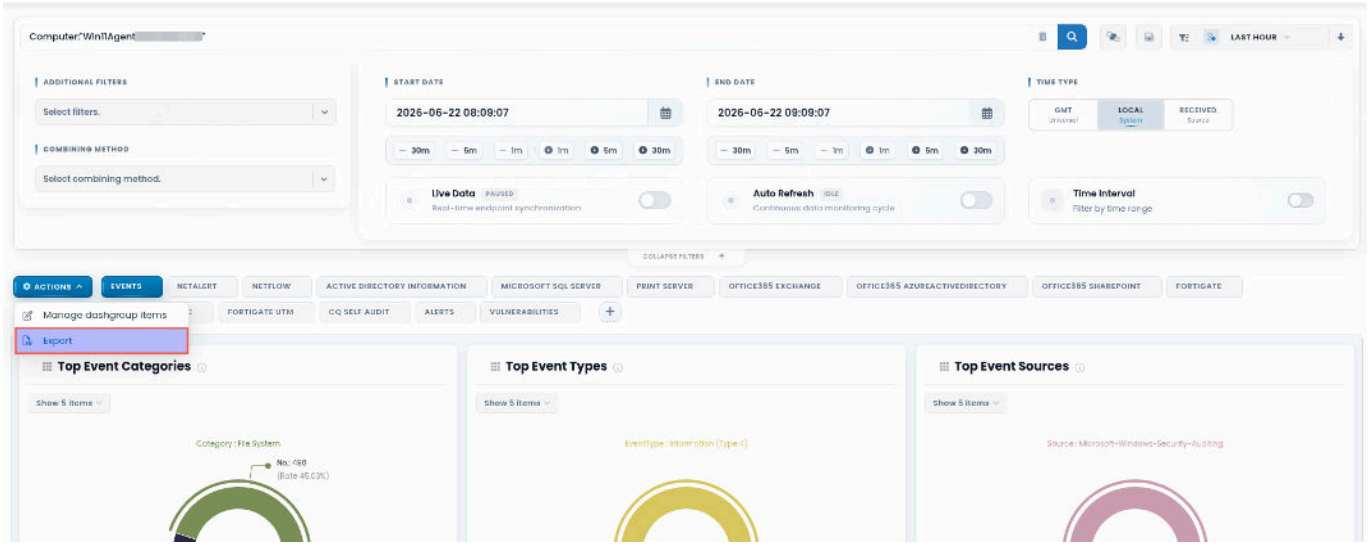
Navigate to Dashboards

- Open the **Dashboards** page and click the expand control to show Search and Filter:



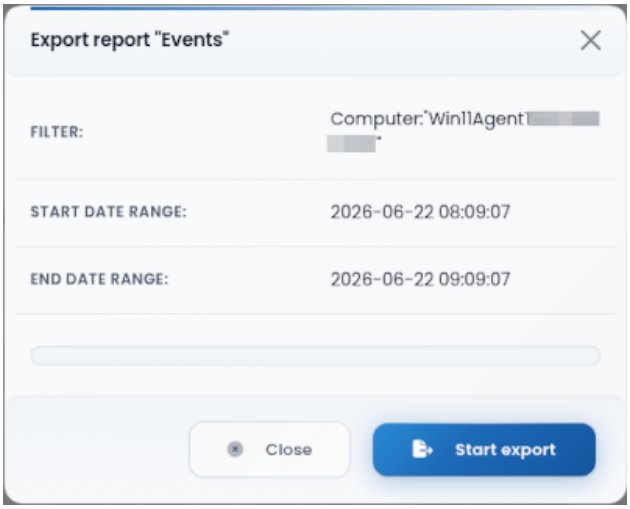
- Choose the dashgroup to export (for example, Events, Network, Alerts) or a custom dashgroup
- Optionally, apply filters (for example, `EventID`, `UserName`, `Computer`) using search and additional filters

Click the **Export** button:

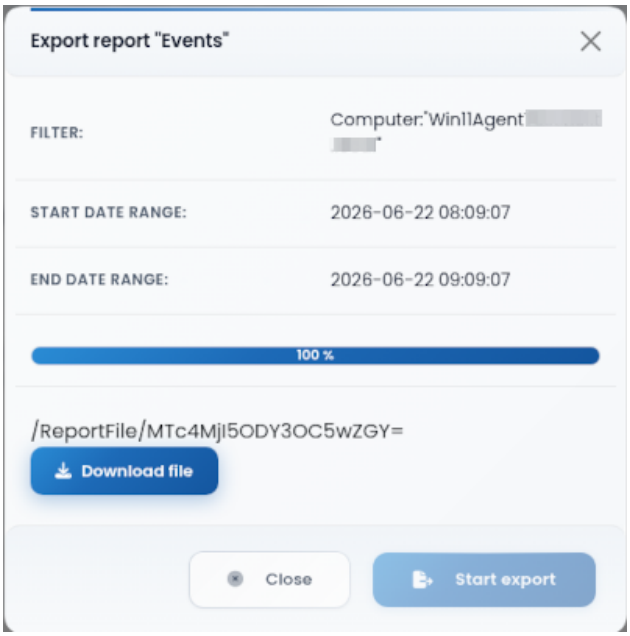


Export the dashgroup

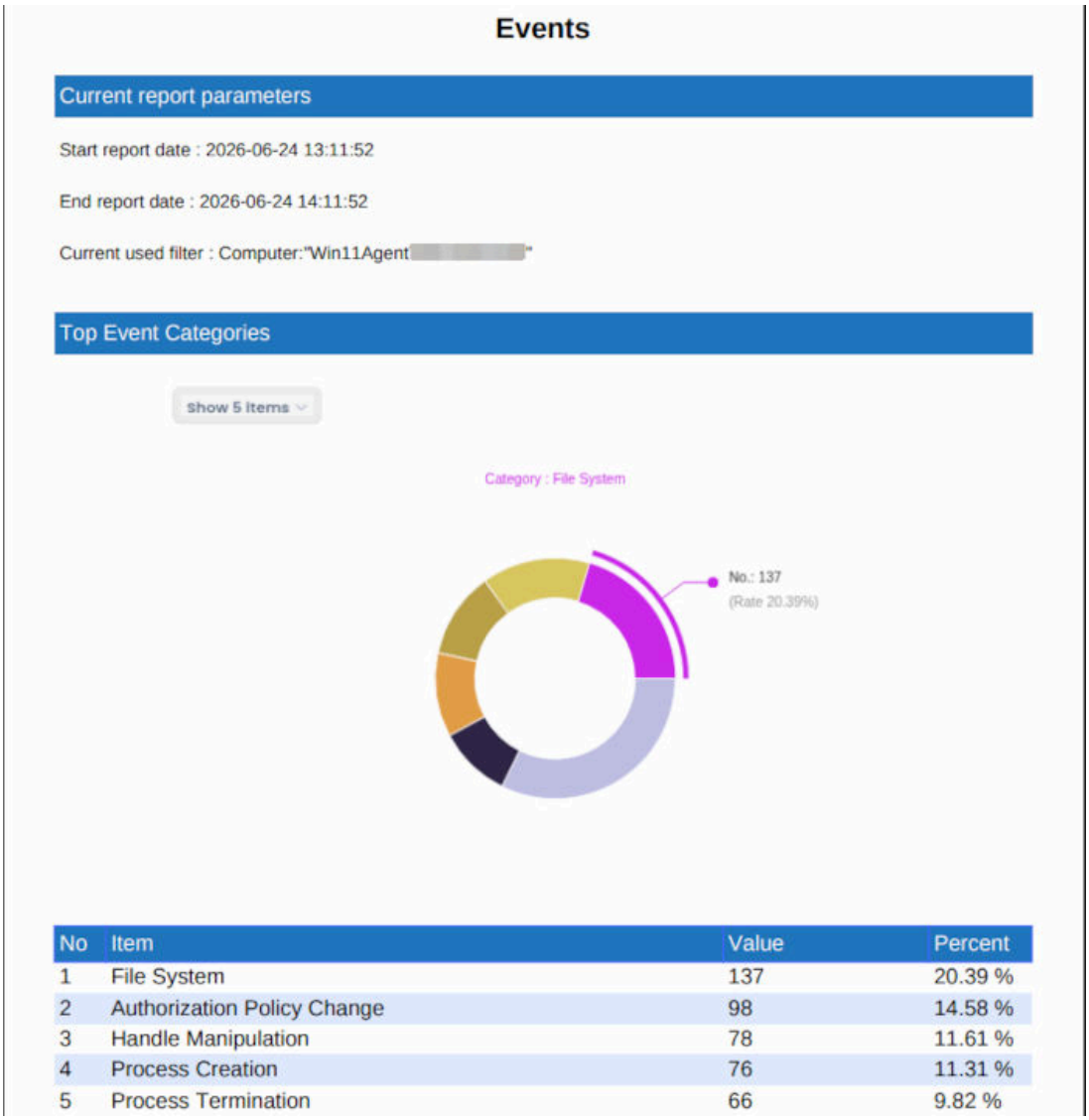
Start the export by clicking **Start export** (or click **Close** to cancel).



When the export completes, click **Download file** to save the PDF locally.



Example of a downloaded PDF report:



Events

Current report parameters

Start report date : 2026-06-24 13:11:52

End report date : 2026-06-24 14:11:52

Current used filter : Computer:"Win11Agent

Top Event Categories

Show 5 items

Category : File System

No.: 137
(Rate 20.39%)

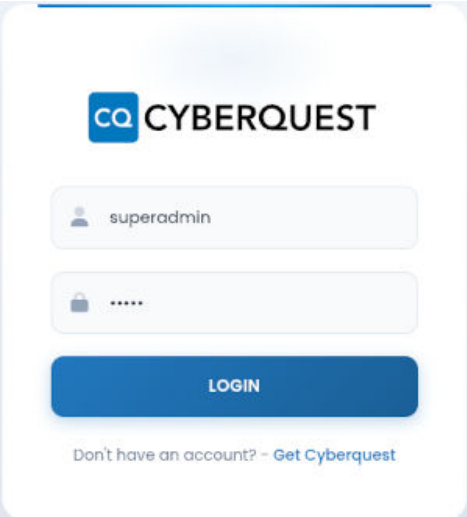
No	Item	Value	Percent
1	File System	137	20.39 %
2	Authorization Policy Change	98	14.58 %
3	Handle Manipulation	78	11.61 %
4	Process Creation	76	11.31 %
5	Process Termination	66	9.82 %

Operations · How to export data from Reports page

Export report results from the Reports page in multiple formats (CSV, XLSX, PDF, HTML, XML, or CQO) after running a report for a selected time range and fields.

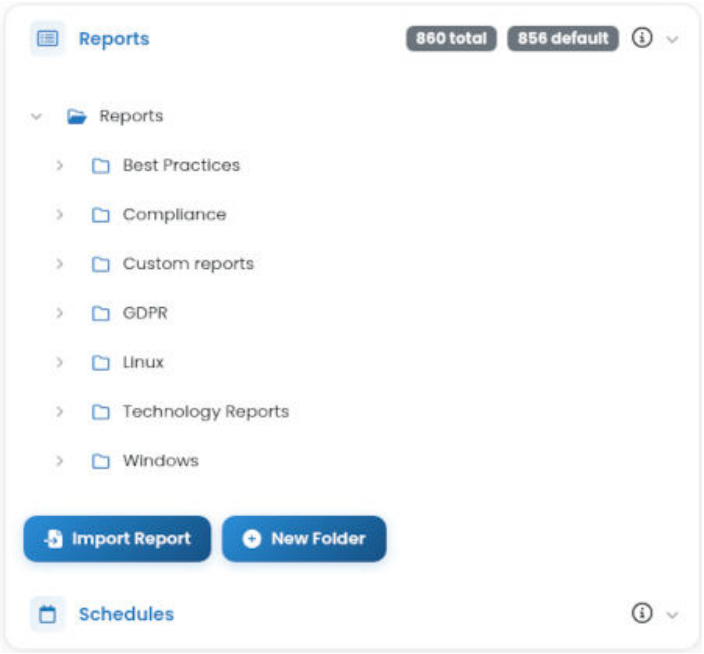
Authentication

To access the web interface, open a browser and enter the application's IP address or DNS name (for example, ***https://CyberquestIPAddress***). The browser redirects to the CYBERQUEST authentication page.



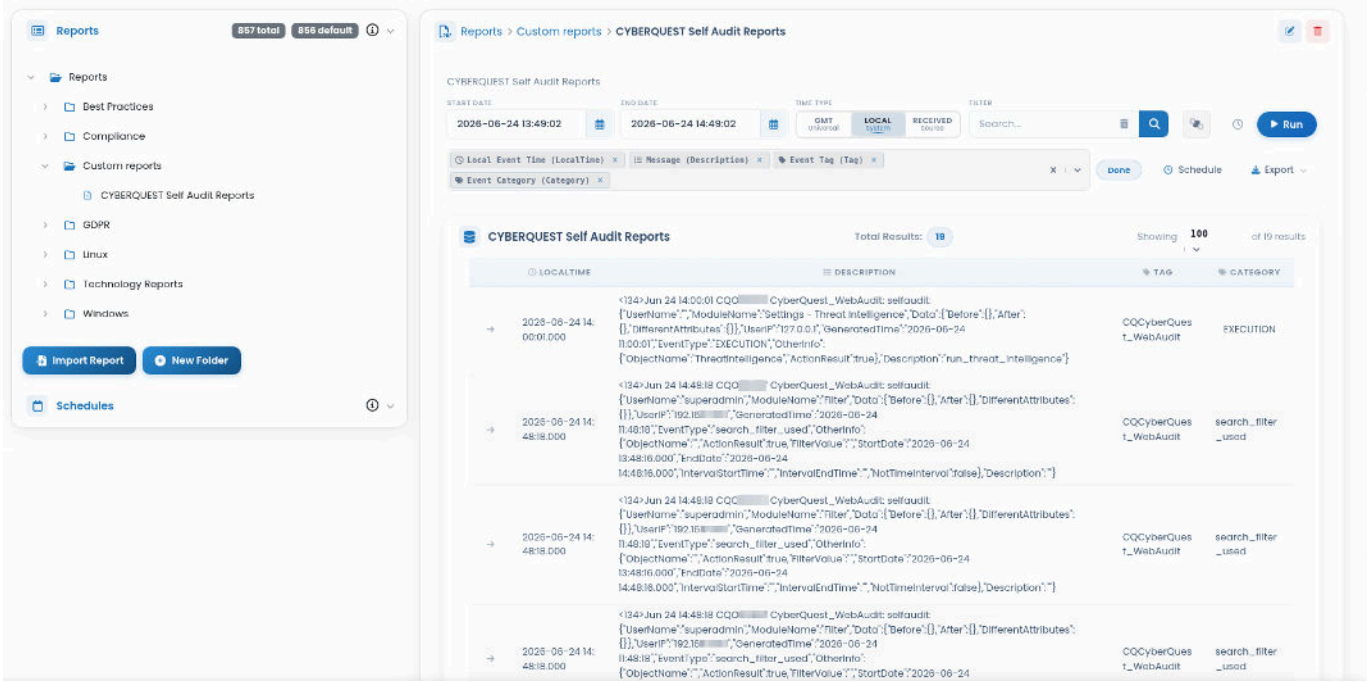
Navigate to Reports

Open the Reports page and select a report (for example, Self Audit Reports) from the **Custom reports** folder.



Execute Report

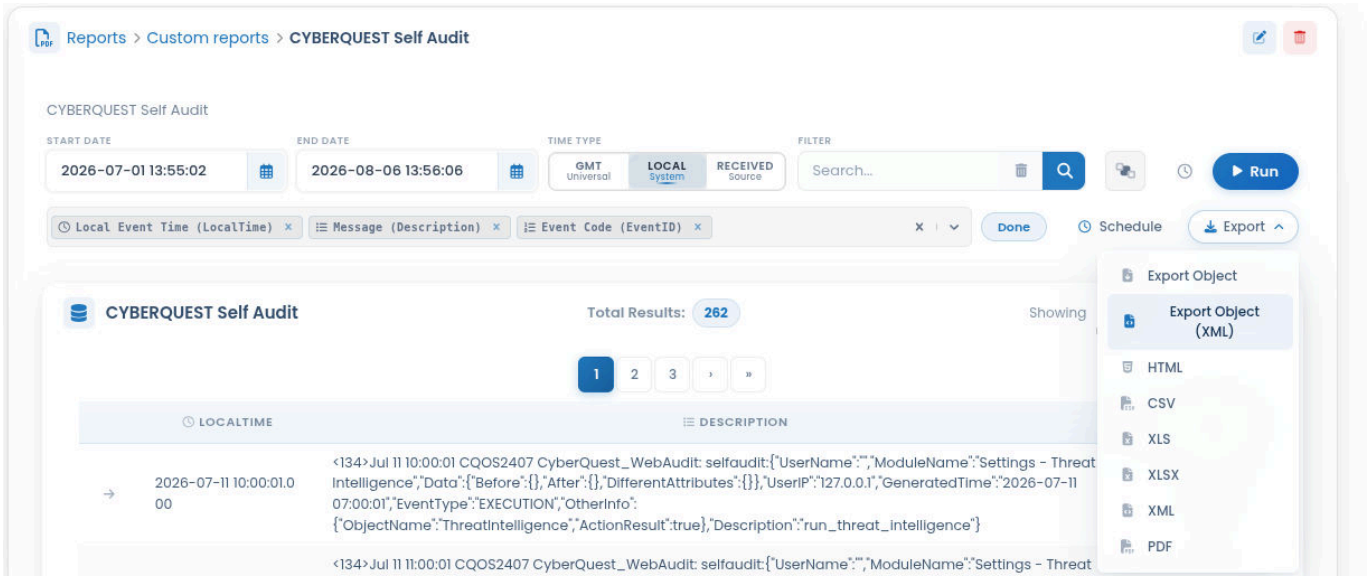
Configure the time interval and output fields, and then click **Execute Report** to generate the report.



- **Start Date** and **End Date** fields define the reporting period.
- The **Items on page** drop-down menu allows selection of the number of items displayed per page (100, 50, or 10).
- Enabling the **Time Interval** checkbox allows selection of specific time ranges for each day within the selected date range.
- A time reference indicator (LocalTime, GMT, or ReceivedTime) is displayed to the right. The selected option determines how time values are interpreted in the report.
- The **Search** field accepts custom queries to limit the data included in the report. This field supports the same syntax used in the Dashboards, Browser.
- Below the Search box, a **field selection** panel is available to customize the report columns. Additional fields can be selected or deselected as needed.
- Reports can also be scheduled with the selected execution options by clicking the ***"Schedule This Report"*** button in the details window.

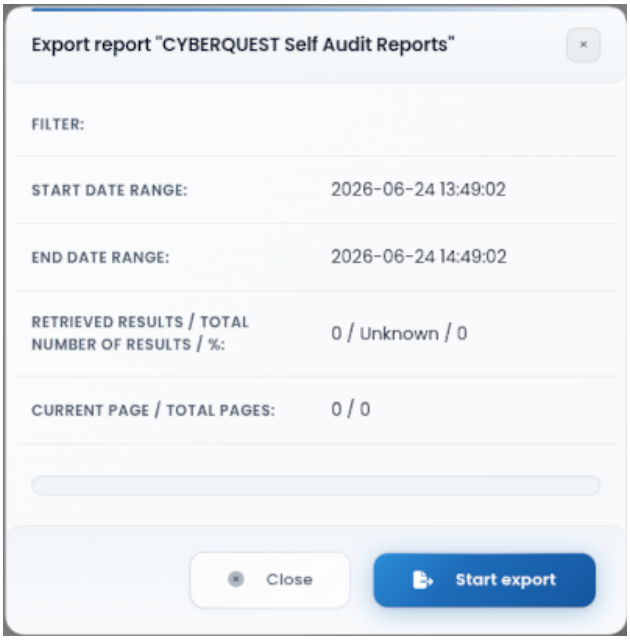
Data export options

Once the report has finished running, select **Export** to choose the export format. Available formats include **CQO**, **Export Object (XML), HTML**, **CSV**, **XLS**, **XLSX**, **XML**, and **PDF**.

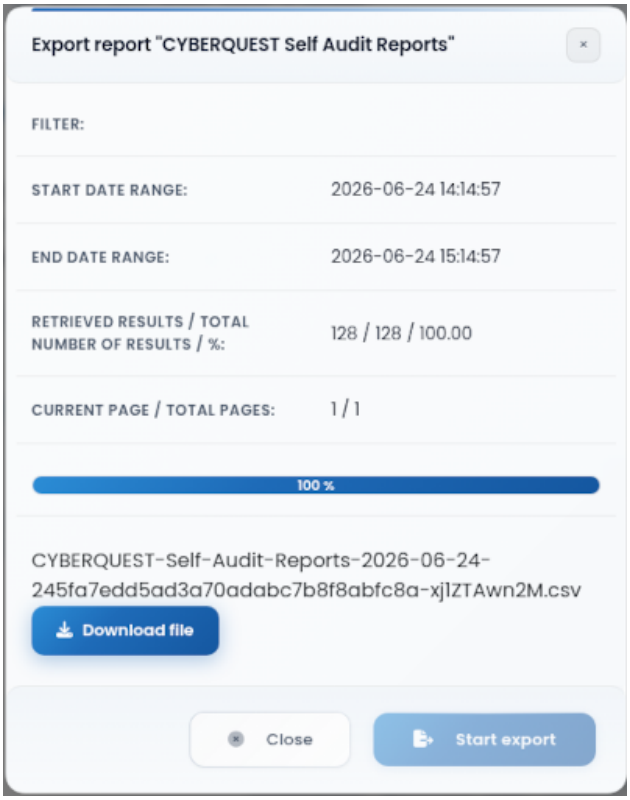


Export the report

Click **Start export** to initiate the export, or **Close** to stop.



After the export finishes, click **Download file** to download the report to the local system.



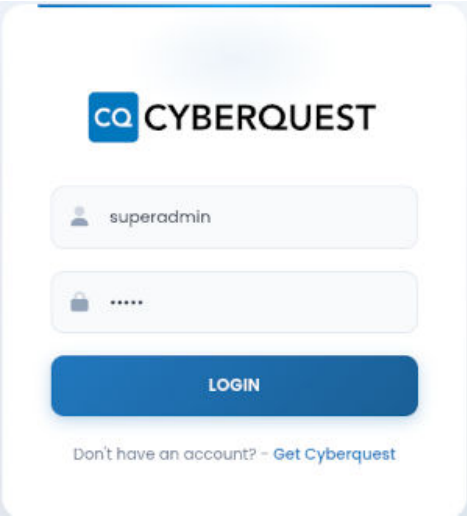
Operations · How to forward alerts to another host

Alert Forwarding to another host adds an extra layer of monitoring and management for critical systems, helping to ensure timely detection and resolution of potential issues.

The following steps explain how to configure alert forwarding:

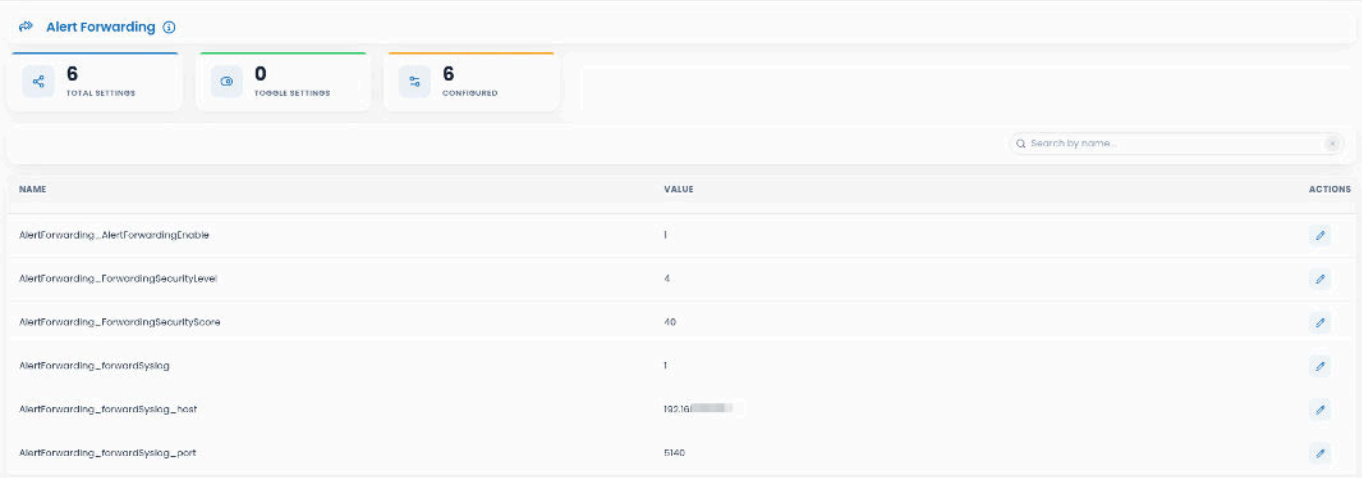
Authentication

To access the web interface, open a browser and enter the application's IP address or DNS name (for example, ***https://CyberquestIPAddress***). The browser redirects to the CYBERQUEST authentication page.



Navigate to Settings

Go to **Settings > Application Settings** and select **AlertForwarding**.



Configure the following parameters:

- **AlertForwarding_AlertForwardingEnable** - set `1` to enable alert forwarding, `0` to disable
- **AlertForwarding_ForwardingSecurityLevel** - minimum security level for alerts to be forwarded
- **AlertForwarding_ForwardingSecurityScore** - minimum security score for alerts to be forwarded
- **AlertForwarding_forwardSyslog** - set `1` to enable Syslog-based forwarding, `0` to disable
- **AlertForwarding_forwardSyslog_host** - destination host (IP or DNS) that receives alerts
- **AlertForwarding_forwardSyslog_port** - destination Syslog port

After saving the settings, restart the Data Correlation service to apply changes.

Go to **Settings > Application Settings > Data Correlation**:



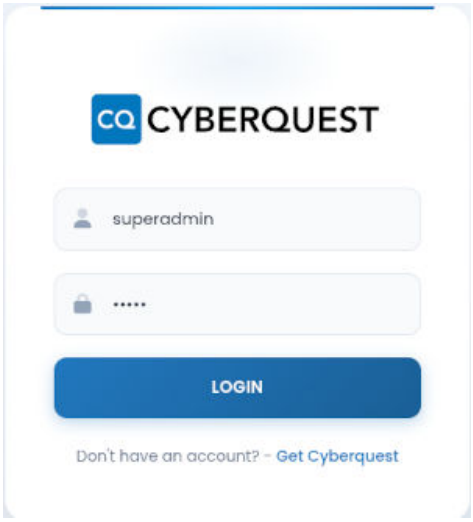
Enter `1` to restart the service. When the restart completes, the value returns to `0`.

Operations · How to forward syslog data

Syslog is a standard protocol used to send event messages between devices and systems. The **DataForwarder** service can forward events to a remote Syslog server (UDP/TCP), or via other formats. The steps below outline how to configure Syslog forwarding and limit which events are sent.

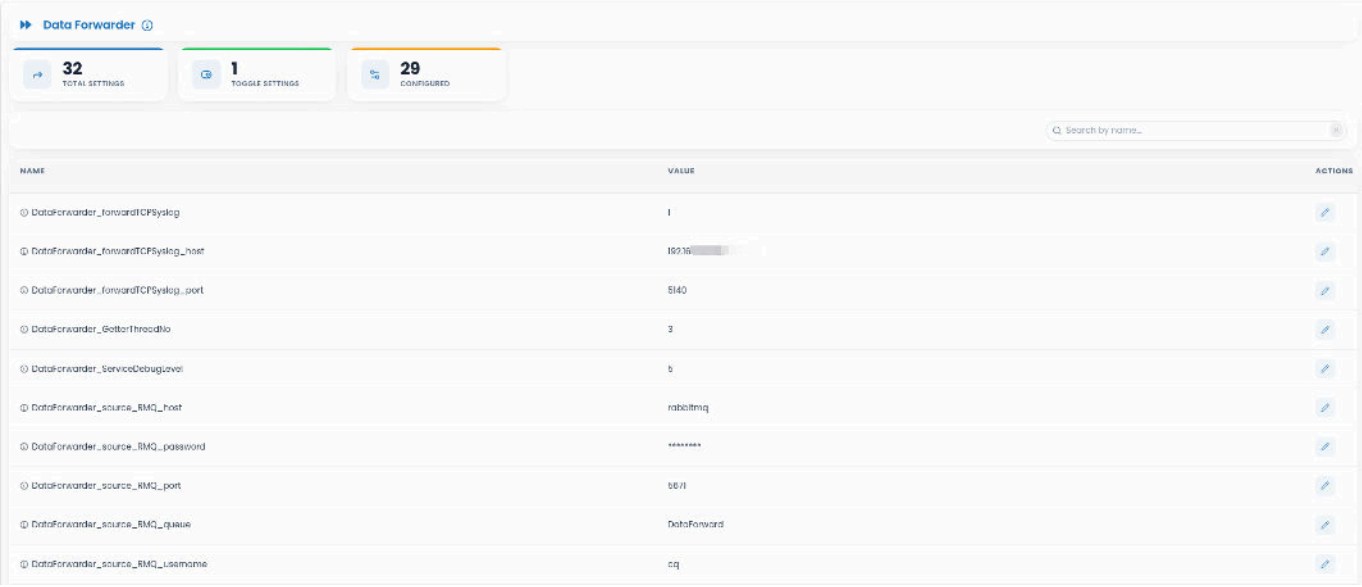
Authentication

To access the web interface, open a browser and enter the application's IP address or DNS name (for example, ***https://CyberquestIPAddress***). The browser redirects to the CYBERQUEST authentication page:



Navigate to Settings

Go to **Settings > Application Settings** and select **DataForwarder**. Configure the following parameters as needed:

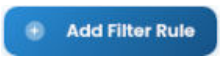


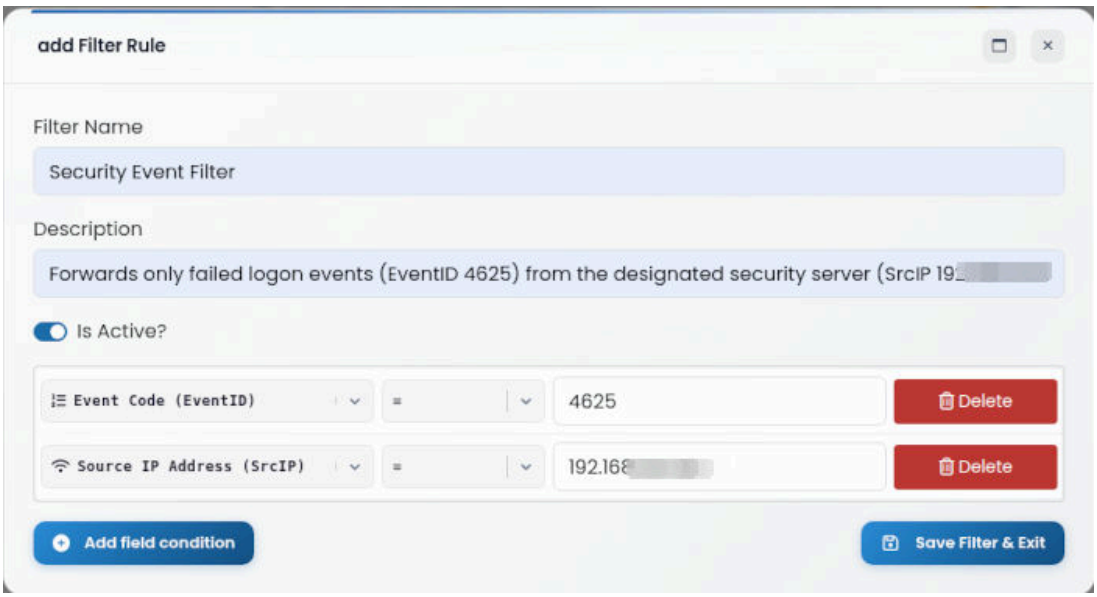
Learn how to configure and adjust the parameters for optimal performance by modifying the **DataForwarder** settings. For detailed instructions, see Adjusting DataForwarder Settings.

Add a Filter Rule

To forward only specific events, create a Filter Rule: go to **Settings > Rules > Filter Rules**.

Click the add button to create a new rule:

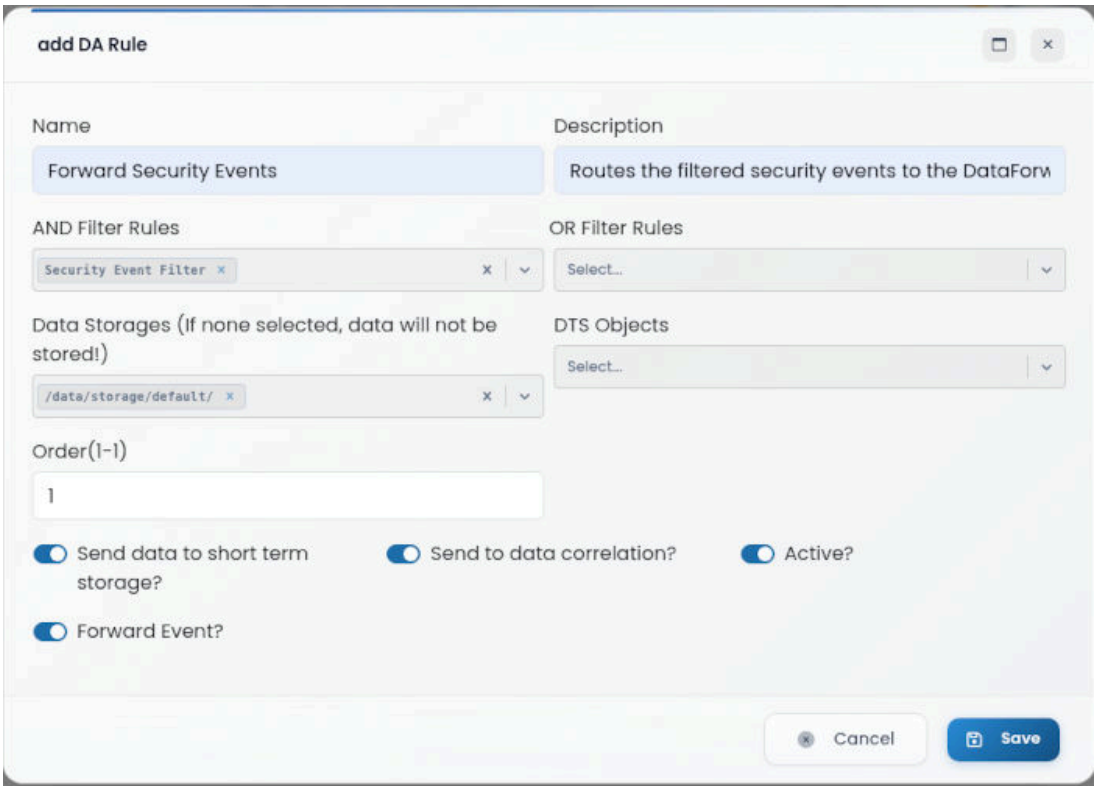




Define conditions that identify the events to forward (for example, `EventID`, `SrcIP`, `DestIP`, `UserName`). Click Save.

Add a DA Rule

Add a DA Rule under **Settings > Rules > DA Rule** to control routing:



- **Send data to short term storage?** - Optionally store events in Online DataStorage for temporary retention.
- **Send to data correlation?** - Optionally route events to the Data Correlation service for analysis and insights.
- **Forward Event?** - Required: Enable to forward events through the DataForwarder to external systems.
- **Active?** - Required: Activate the DA Rule to make it operational.

Click Save.

How to identify forwarded events

- Syslog events are forwarded without modification.
- Non-Syslog events are reformatted as Syslog; the DataServer assigns a tag and computer from the description.
- Events without description are sent as JSON.

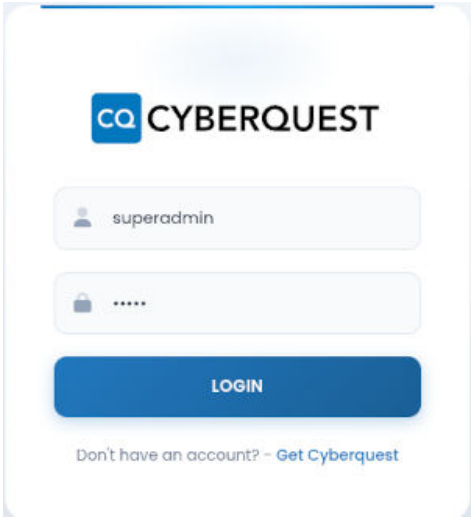
Operations · How to create a new dashboard, dashgroup and view data

A CYBERQUEST dashboard is a graphical view of events. Access it from the **Dashboards** module after sign-in or via the Dashboards button in the top-left of the web interface.

How to create a new dashboard

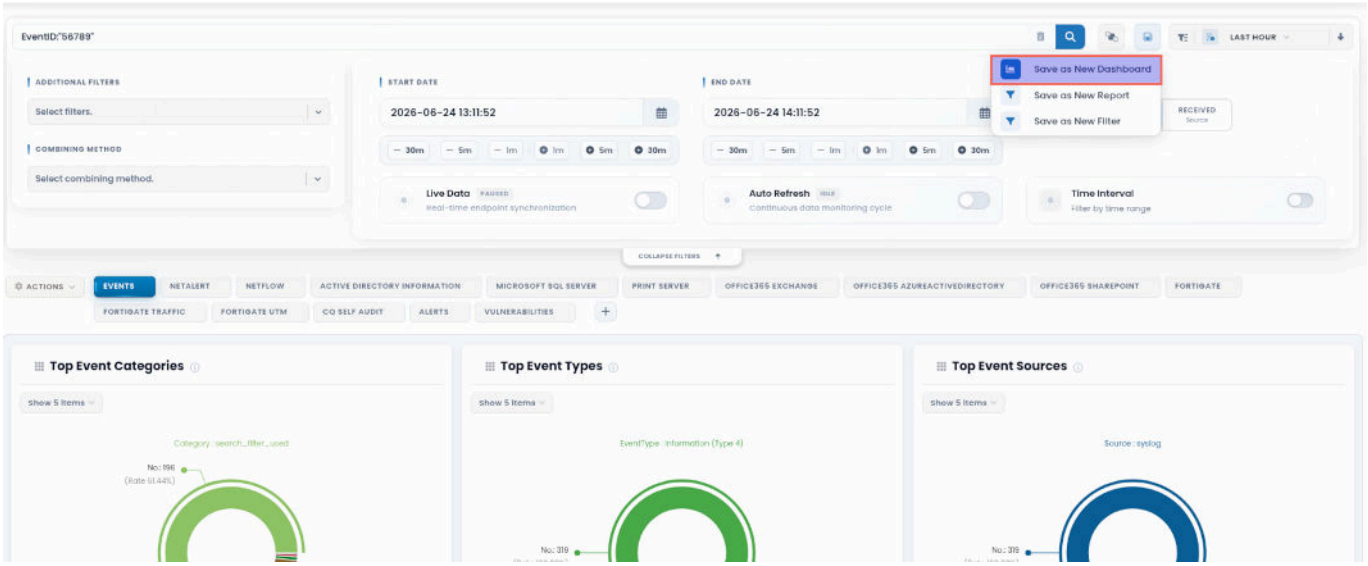
Authentication

To access the web interface, open a browser and enter the application's IP address or DNS name (for example, ***https://CyberquestIPAddress***). The browser redirects to the CYBERQUEST authentication page:



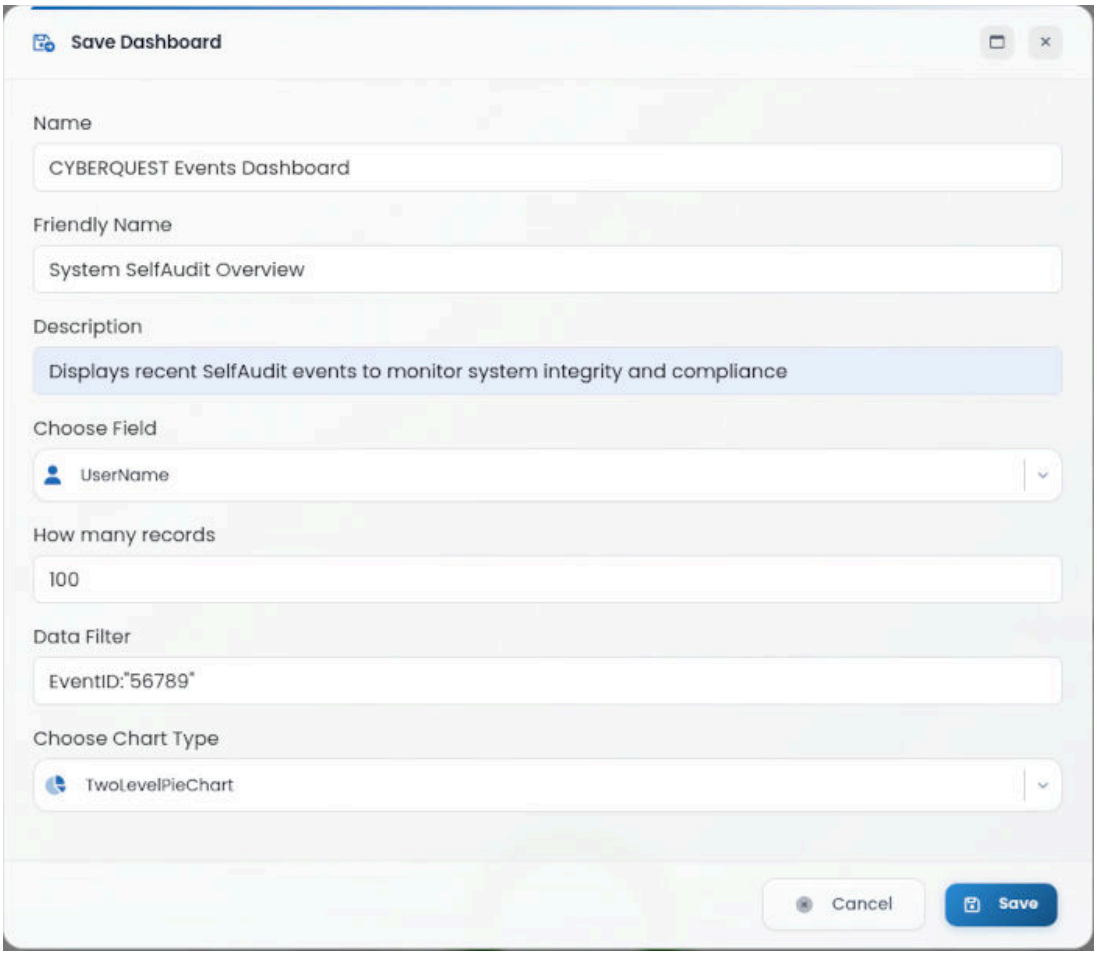
Navigate to Dashboards

Open the Dashboards page. Apply a filter for the data of interest (for example: `EventID:"56789"`). Save it as a dashboard: click **SAVE OPTIONS** > **Save as New Dashboard**.



Complete the form

Complete the form and click Save:



Name: The name of the new Dashboard.

Friendly Name: Display label shown in the Dashboards interface for easy recognition.

Text: Brief description of the dashboard's purpose or content.

Choose Field: Select the field by which the data will be aggregated in the visualization.

How many records: Specify the number of top items to display in the dashboard.

Data Filter: Query that determines which data populates the dashboard (automatically pre-filled from the current filter).

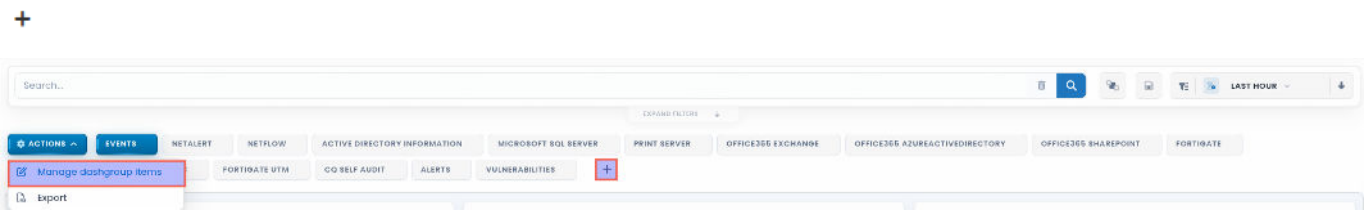
Choose Chart Type: Select the type of visualization to display.

How to create a new dashgroup

A dashgroup is the main display area for dashboards. When a user logs in, they will see dashgroups assigned to their profile. By selecting a dashgroup, the user can view all dashboards included within it. Follow these steps to create a new dashgroup:

Add dashgroup

On the Dashboards page, click **MANAGE DASHGROUP ITEMS** or the plus button:



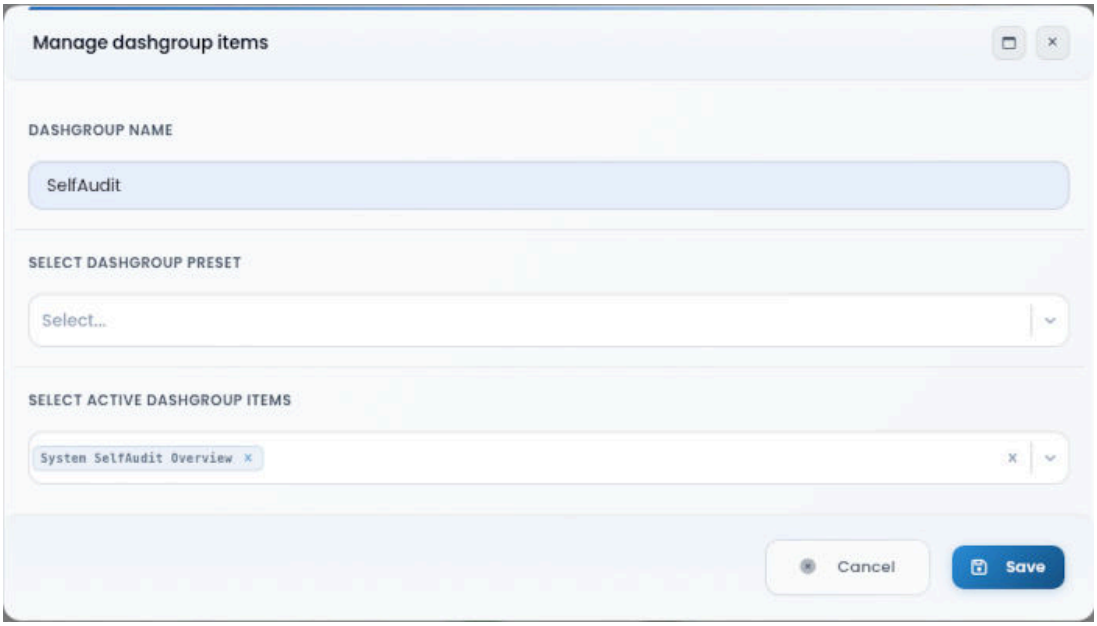
Complete the form

Complete the form and click Save:

Dashgroup name: Enter a name for the dashgroup.

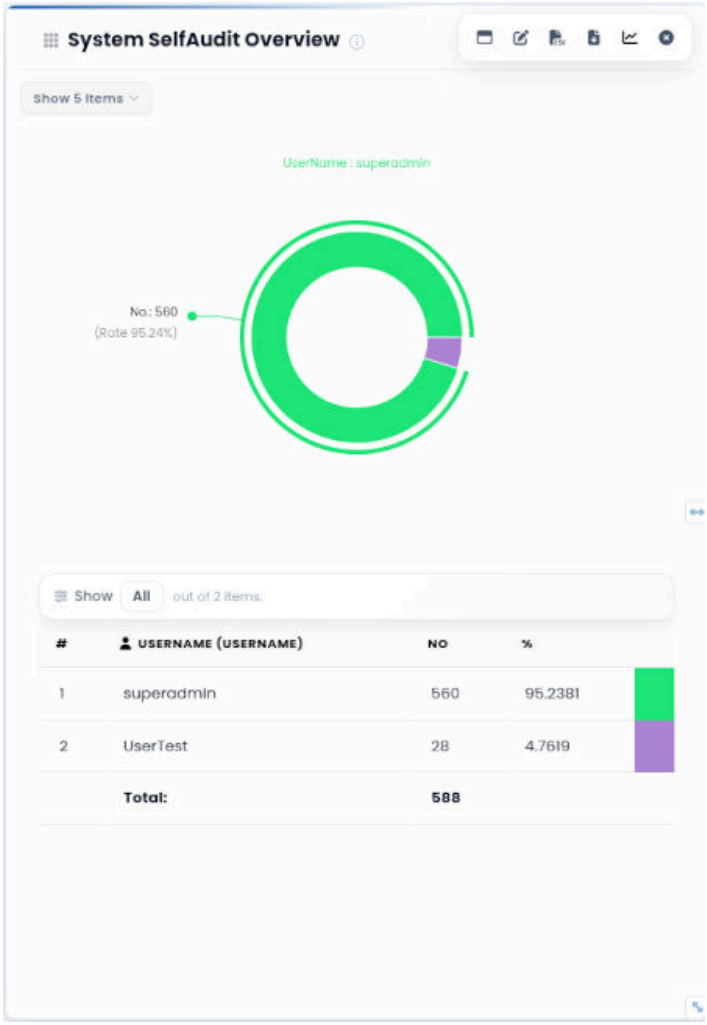
Select dashgroup preset: (Optional) Choose a layout or preset to apply.

Select active dashgroup items: Dashboards to include in this dashgroup.



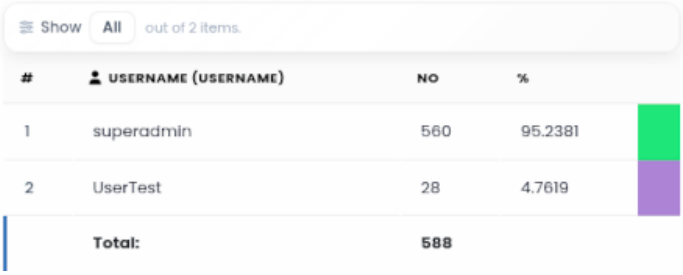
How to view data from a dashboard

The new dashboard appears on the Dashboards page.



Quick actions on a dashboard:

- *Maximize/Minimize* - Expand the dashboard to full screen or restore it to its original size.
- *Edit Dashboard* - Modify and update the saved dashboard settings.
- *Explain* - Sends the dashboard to the AI Chat Assistant for explanation (available only if enabled in **Settings > Chat Config**).
- *Export CSV* - Export the displayed items (limited by the "How many records" setting).
- *Export Dashboard Object* - Save the dashboard configuration in the proprietary format.
- *Graph selection* - Temporarily change the chart type for the current view (does not alter the saved dashboard).
- Show items - Control how many entries are displayed below the chart.



Operations · How to manage collect CSV Files

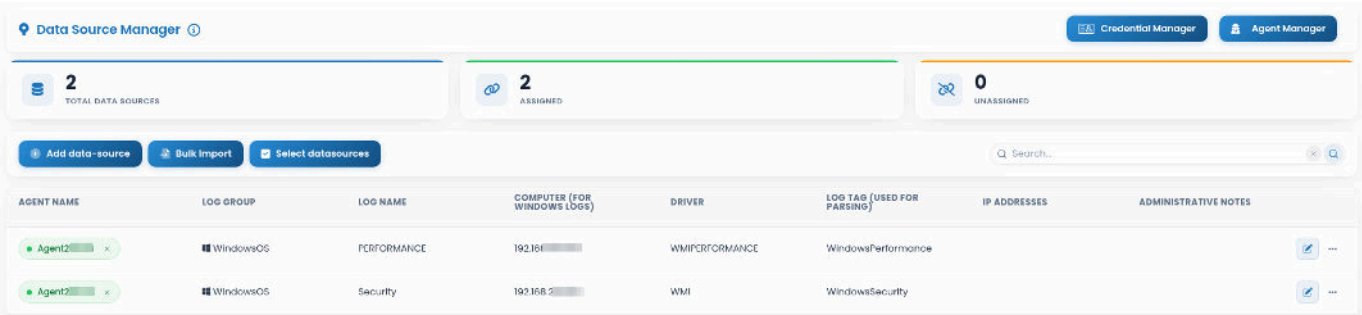
This page explains how to gather and process events from CSV files for analysis or forwarding.

Navigate to Settings

Log in to the CYBERQUEST web interface with an account with administrative rights.

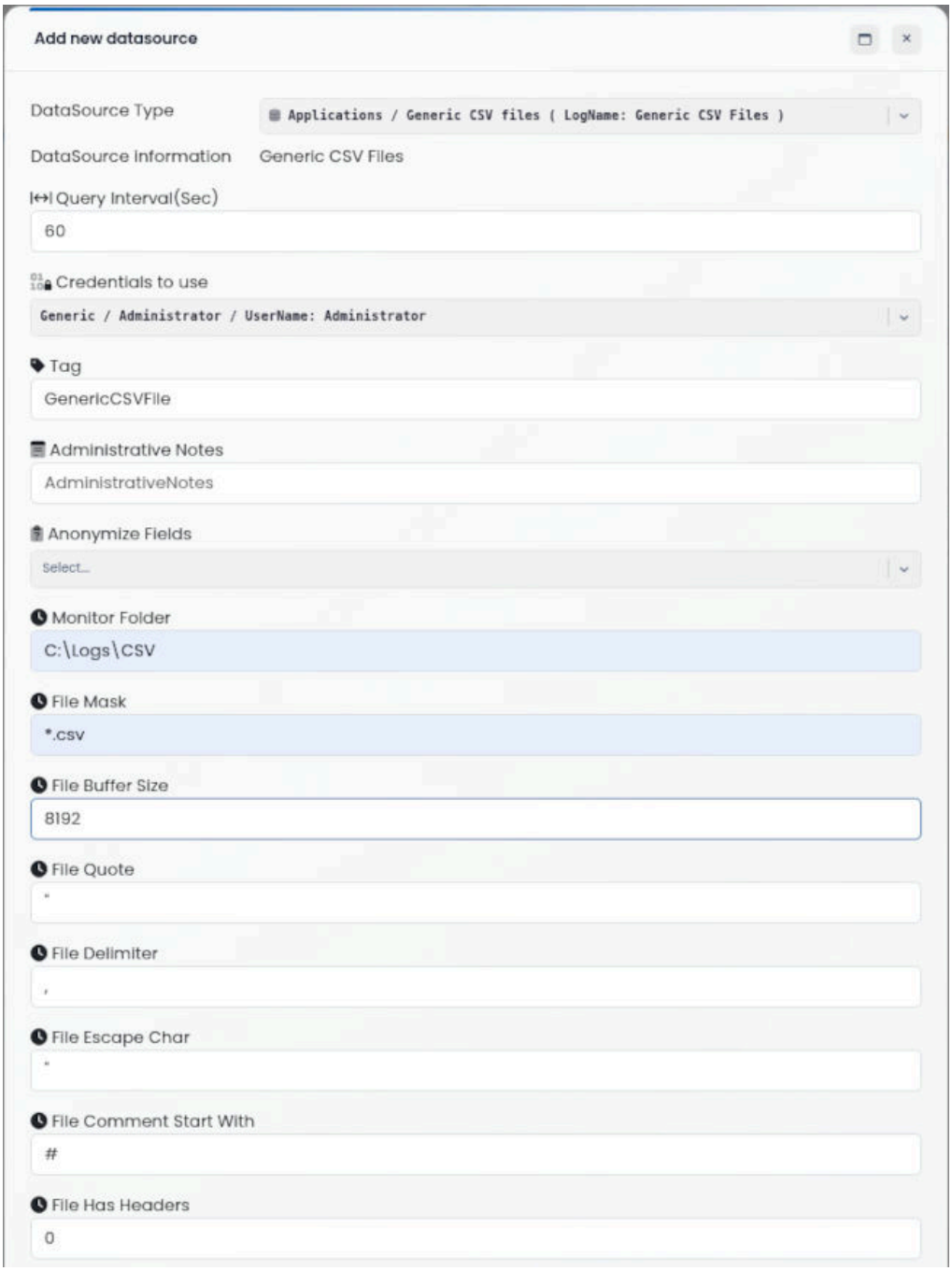
Navigate to "**Settings** > **Management** > **Data Source Manager**".

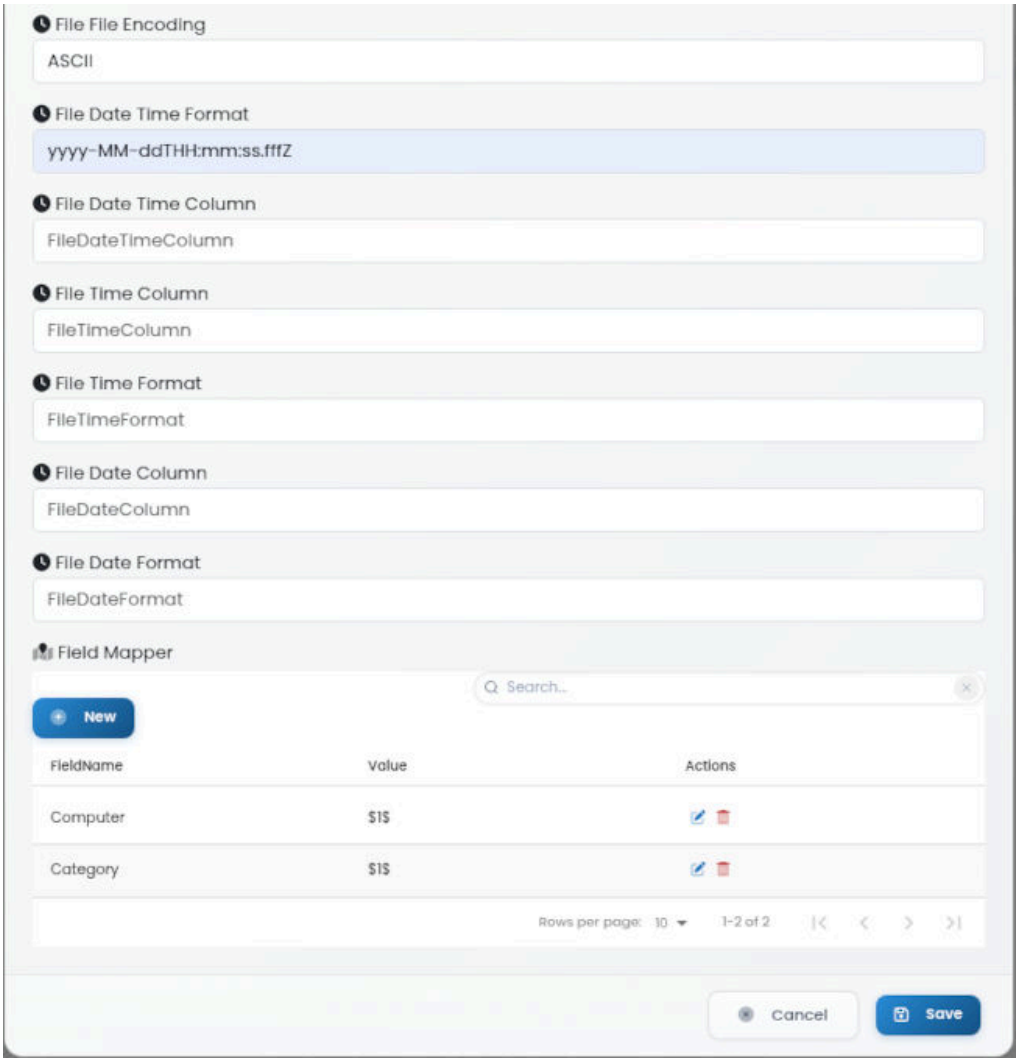
This page contains all the data sources added in the CYBERQUEST application.



Complete the form

Press the "ADD DATA-SOURCE" button and complete the following form:


Add new datasource
DataSource Type
Applications / Generic CSV files (LogName: Generic CSV Files)
DataSource Information
Generic CSV Files
Query Interval(Sec)
60
Credentials to use
Generic / Administrator / UserName: Administrator
Tag
GenericCSVFile
Administrative Notes
AdministrativeNotes
Anonymize Fields
Select...
Monitor Folder
C:\Logs\CSV
File Mask
*.csv
File Buffer Size
8192
File Quote
"
File Delimiter
,
File Escape Char
"
File Comment Start With
#
File Has Headers
0



DataSource Type: Select **Applications / Generic CSV files** as the data source type.

DataSource Information: Automatically populated with details about the selected data source.

Query Interval: Defines how often the folder is scanned for new or updated files. The default interval is **60 seconds**.

Credentials to use: Select credentials if accessing a network share (leave empty for local paths)

Tag: Automatically filled in with a default identifier, which can be customized if needed.

Administrative Notes: Optional field for adding notes or details about the data source.

Anonymize Fields: Select specific fields to anonymize, if required, for data privacy.

Monitored folder: The monitored folder is the specified file path that the system continuously observes for changes.

**File Mask: **Specify the file pattern to include.

File Buffer Size: Define the buffer size (in bytes) used when reading files.

File Quote: Specify the quote character used in the CSV file (e.g., `"`)

File Delimiter: Field delimiter.

File Escape Char: Set the field separator character.

File Comment Starts With: Comment prefix to ignore lines (optional).

File Has Headers: Indicates the first row contains column headers.

File Encoding: Character encoding.

File Date Time Format: Combined date/time format if a single column contains both.

File Date Time Column: Column index or name containing combined date/time.

File Time Column: Column index or name for time (if separate).

File Time Format: Time format.

File Date Column: Column index or name for date (if separate)

File Date Format: Date format.

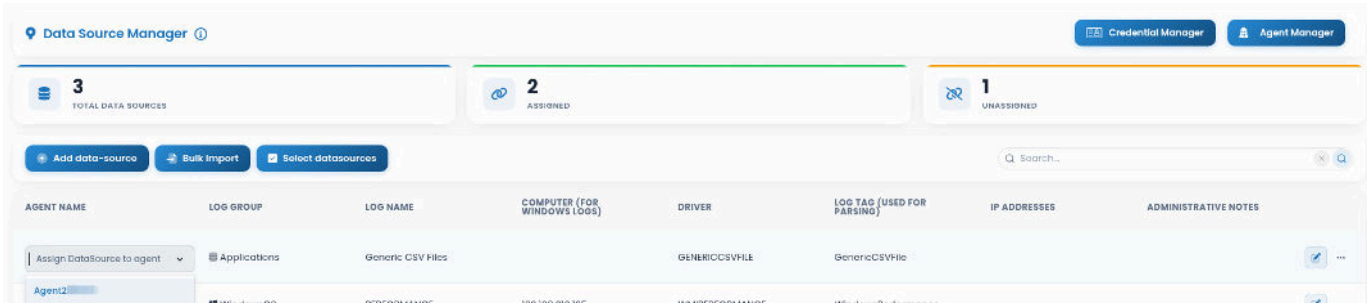
Field Mapper: Map CSV columns to CYBERQUEST fields. Add custom fields with the New button:



Click the “Save” button to save the data source.

Assign the CYBERQUEST agent

The next step is to assign the CYBERQUEST agent to this data source. Choose the agent that has access to the monitored folder.



Actions menu

To edit the data source, click Edit



. This process is almost identical to adding a data source.

Clone



: Clone the data source.

Delete: remove the data source from the list.

Operations · How to collect Oracle audit logs

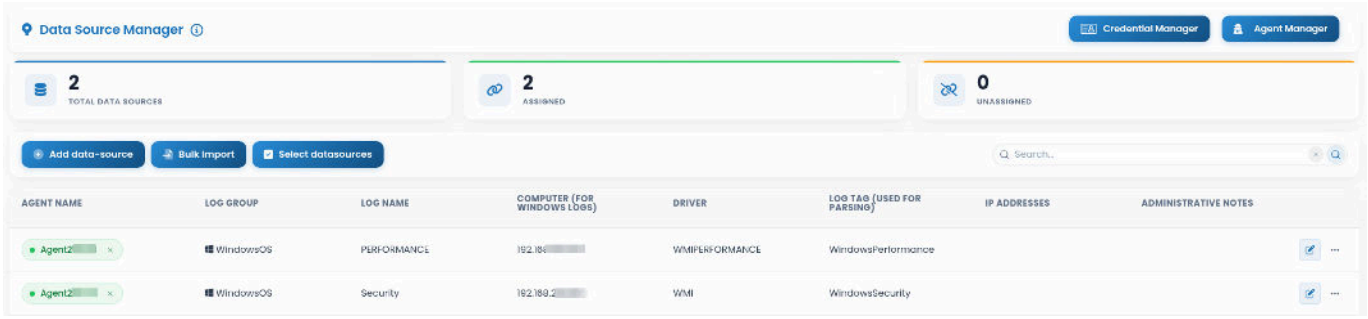
This page describes how to collect audit logs from Oracle databases.

Navigate to Settings

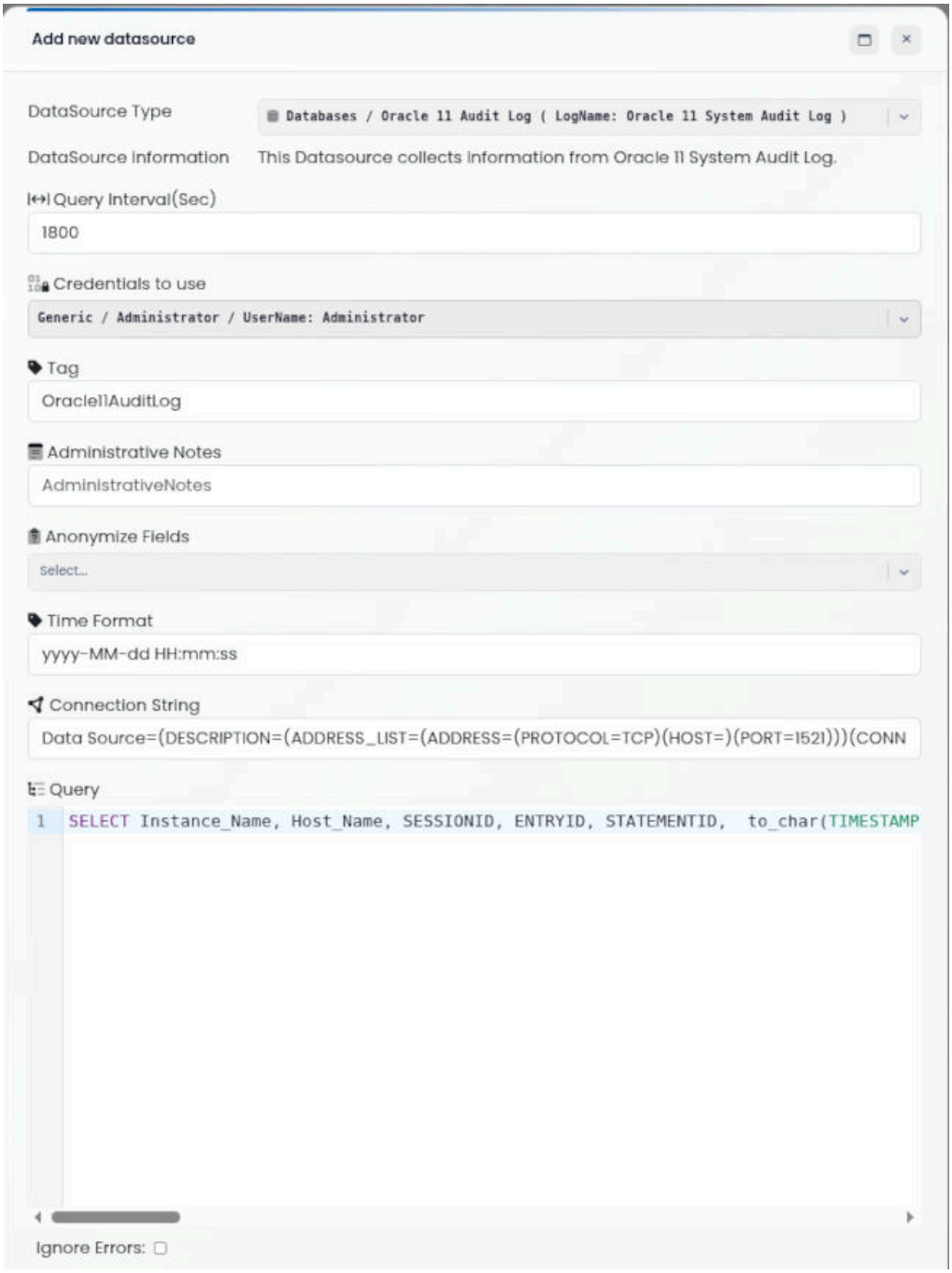
Log in to the CYBERQUEST web interface with an account with administrative rights.

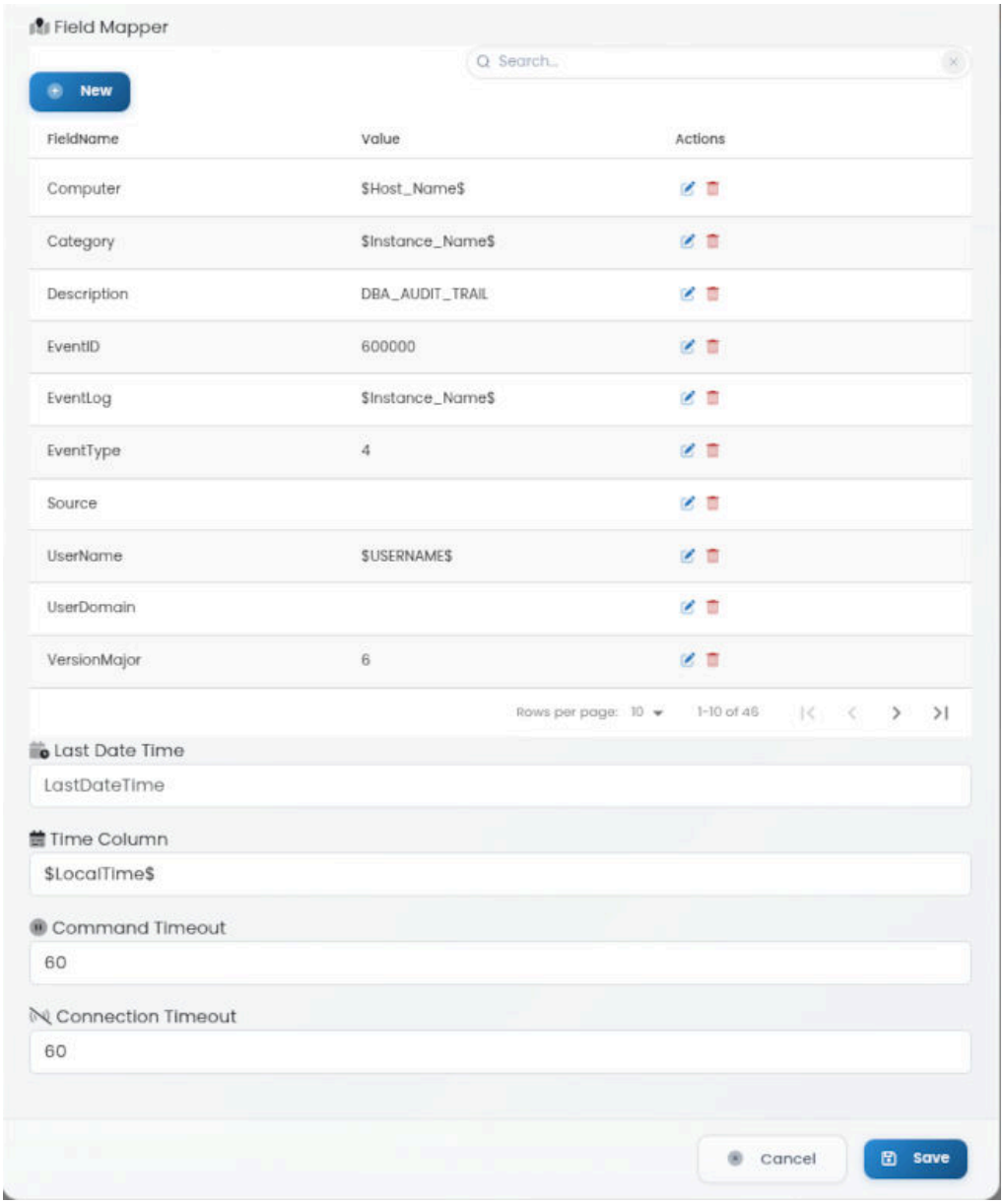
Navigate to **Settings > Management > Data Source Manager**.

This page contains all data sources added in the CYBERQUEST application.



Click **ADD DATA-SOURCE** to create and configure a new data source.





DataSource Type: Select `Database / Oracle 11 Audit Log` or `Database / Oracle 12 Audit Log` based on the Oracle version

DataSource Information: Auto-populated information about the data source

Query Interval: How often the query runs (default: 1800 seconds / 30 minutes)

Credentials to use: Select Oracle credentials from the list (user with access to audit data)

Tag: Auto-filled identifier, can be customized

Administrative Notes: Optional notes for administrators

Anonymize Fields: Select fields to anonymize (optional)

Time Format: Time format used by the audit timestamp

Connection String: Database connection string (for example, `HOST=...;PORT=...;SERVICE_NAME=...`)

Query: SQL query used to extract audit data (adjust to the audit schema/structure)

Field Mapper: Map query result columns to CYBERQUEST fields. Add custom mappings with the New button:



Last Date Time: Starting point for collection

Time Column: Column name containing the audit timestamp

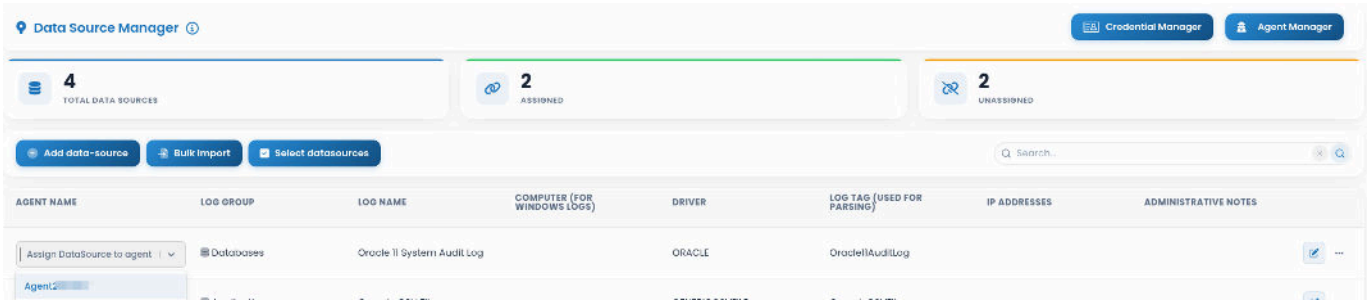
Command Timeout: Seconds to wait for query execution before timeout (default: 60 seconds)

Connection Timeout: Seconds to wait when establishing the connection (default: 60 seconds)

Click the “Save” button to save the data source.

Assign the CYBERQUEST agent

Assign a CYBERQUEST agent to this data source. Choose the agent that has network access to the Oracle server.



Actions menu

To edit the data source, click Edit



. This process is almost identical to adding a data source.

Clone



: Clone the data source.

Delete: remove the data source from the list.

Operations · How to manage credentials

Credential entries specify the accounts that agents use to collect data. For a Windows agent, the account must have administrative rights.

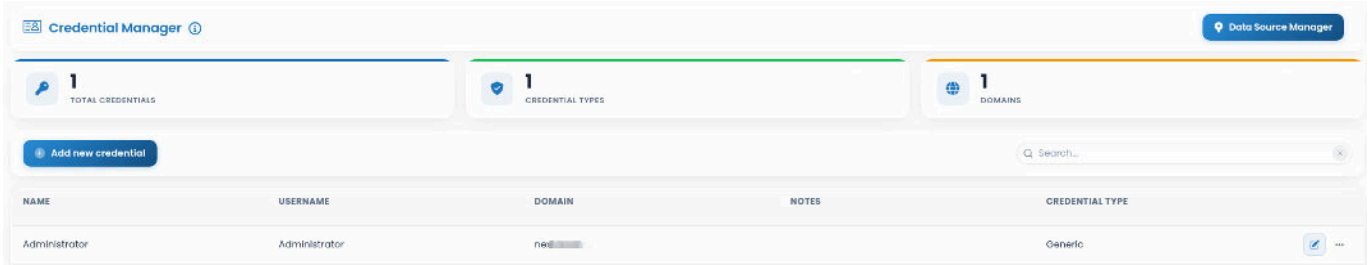
Navigate to Settings

Log in to the CYBERQUEST web interface with an account with administrative rights.

Navigate to **Settings > Management > Credential Manager**:

On this page, credentials for collection agents can be created, edited, or deleted.

The Search function on the right side of the page filters existing credentials.



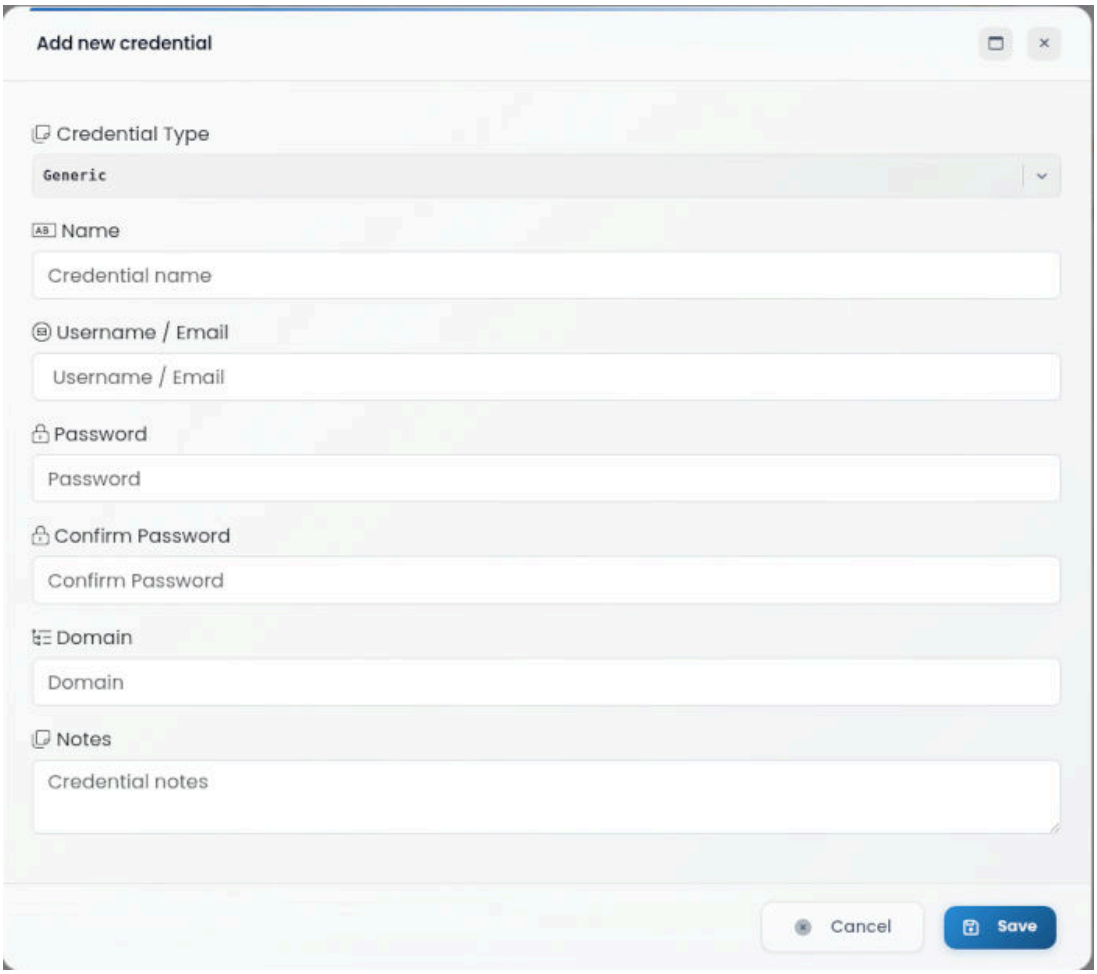
- To edit a credential, click Edit

  . This process is almost identical to adding credentials.
- Copy GUID: Copies the unique identifier (GUID) of the credential.
- Delete removes a credential from the list.

Add new credential

Select **ADD NEW CREDENTIALS** and complete the form:



Name: Identifier for the credential set (multiple sets can exist)

Username/Email: Account name or email address

Password: Account password

Confirmation Password: Repeat the password to confirm

Domain: Domain name when using a domain account (leave empty for local accounts)

Notes: Optional details about the credential usage or scope

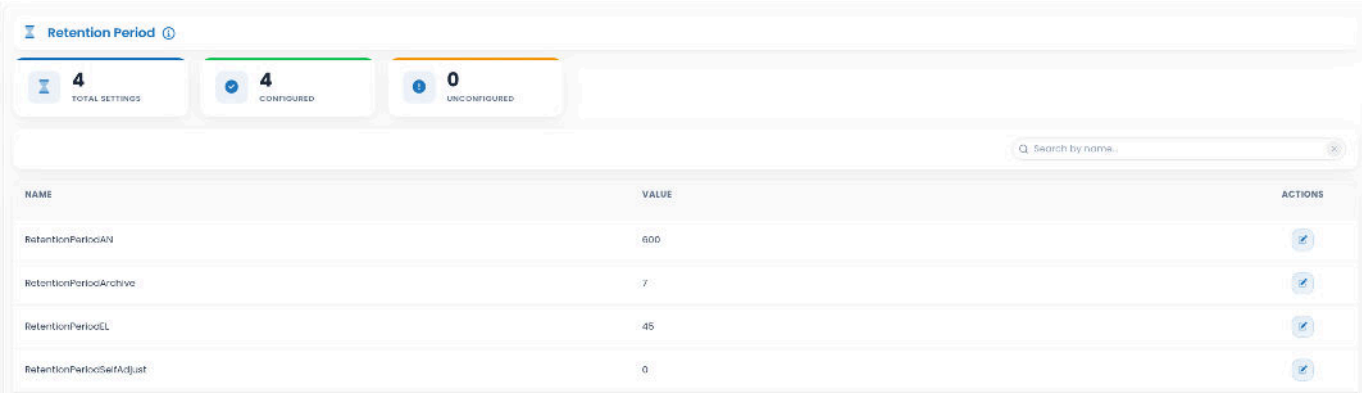
Click **Save** to create the credential, or **Cancel** to discard changes.

Operations · How to manage CYBERQUEST data

In CYBERQUEST, data is stored in two locations:

- Online DataStorage (short-term storage)
- Data storage (archive / long-term storage)

Adjust the data retention period under **Settings > Application Settings > Retention Period**.



Parameters:

- **RetentionPeriodAN:** Retention time for data in Data Analyzer (deprecated)
- **RetentionPeriodArchive:** Retention period in days for the archive database
- **RetentionPeriodEL:** Retention period in days for the online database (Online DataStorage)
- **RetentionPeriodSelfAdjust:** `1` (enabled) or `0` (disabled).
  - When set to `1`, the online retention (**RetentionPeriodEL**) is automatically adjusted based on available storage.
  - When set to `0`, retention remains fixed and CYBERQUEST collects data until disk space is exhausted; new data is no longer collected when the disk is full.

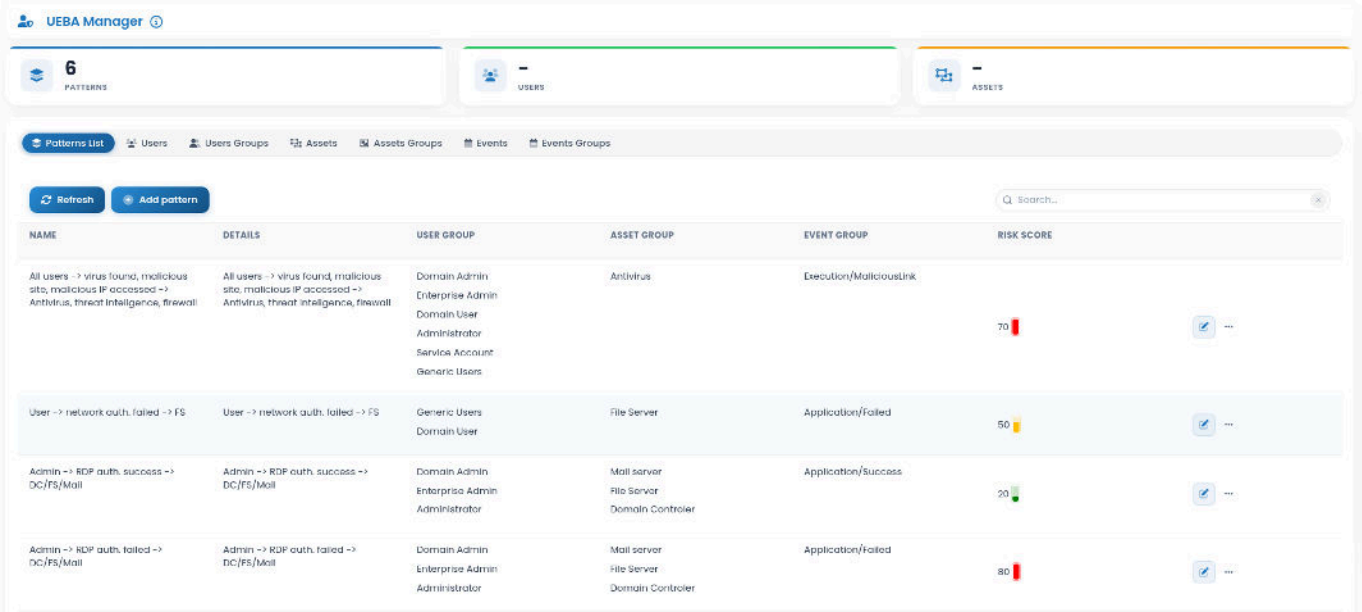
To adjust the retention period of Online DataStorage, see: How to delete events older than 6 months - Delete from online database.

To delete data from the archive (offline database), see: How to delete events older than 6 months - Delete from archive (offline) database.

Operations · How to manage Ueba

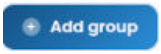
UEBA Manager configures membership of users, assets, and events in related groups (UserGroup, AssetGroup, EventGroup) used for behavioral analytics and risk scoring.

To access the page, go to **Settings > Management > UEBA Manager**.

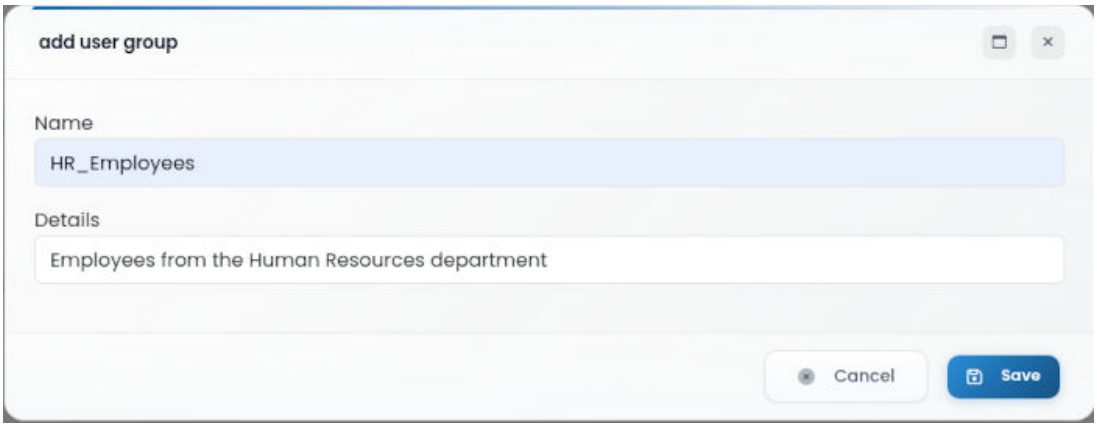


User groups

Create a group in **Users Groups** by clicking the add button:



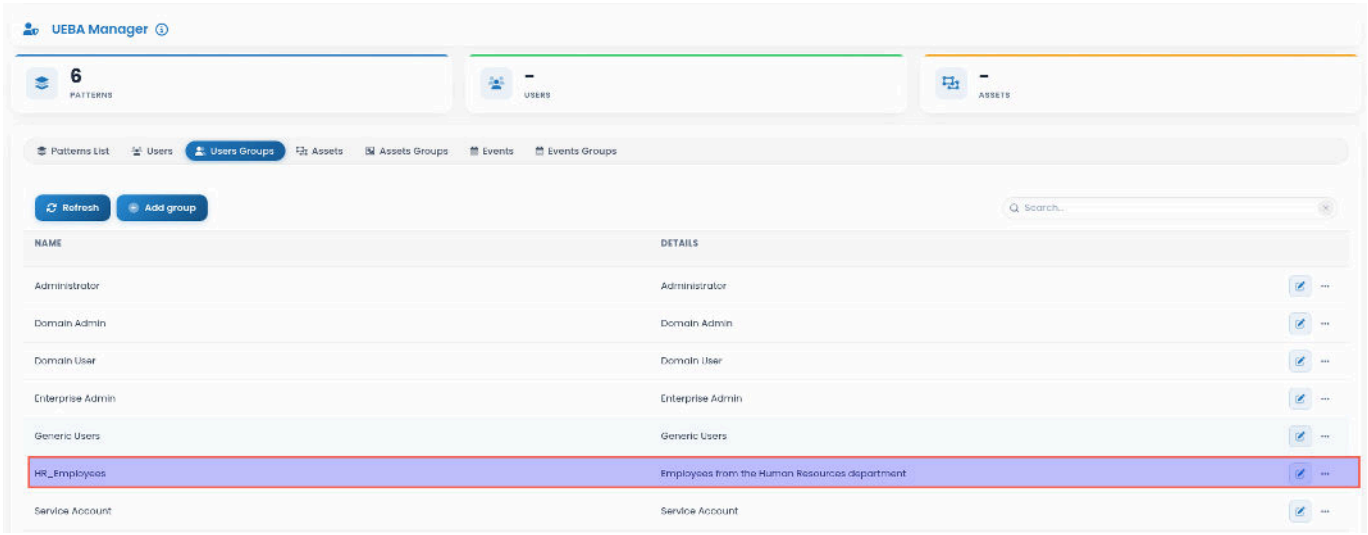
.



- **Name:** Name that identifies the user group
- **Details:** Additional details about the group

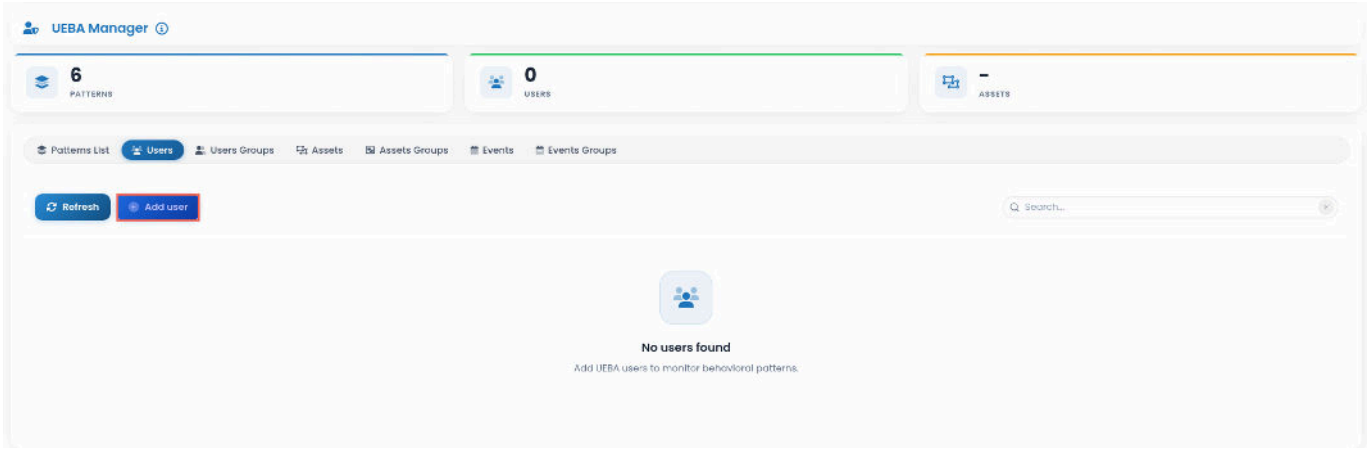
Click **Save** to create the user group, or **Cancel** to discard.

The **Users Groups** view lists existing groups and provides options to edit, update, or delete:

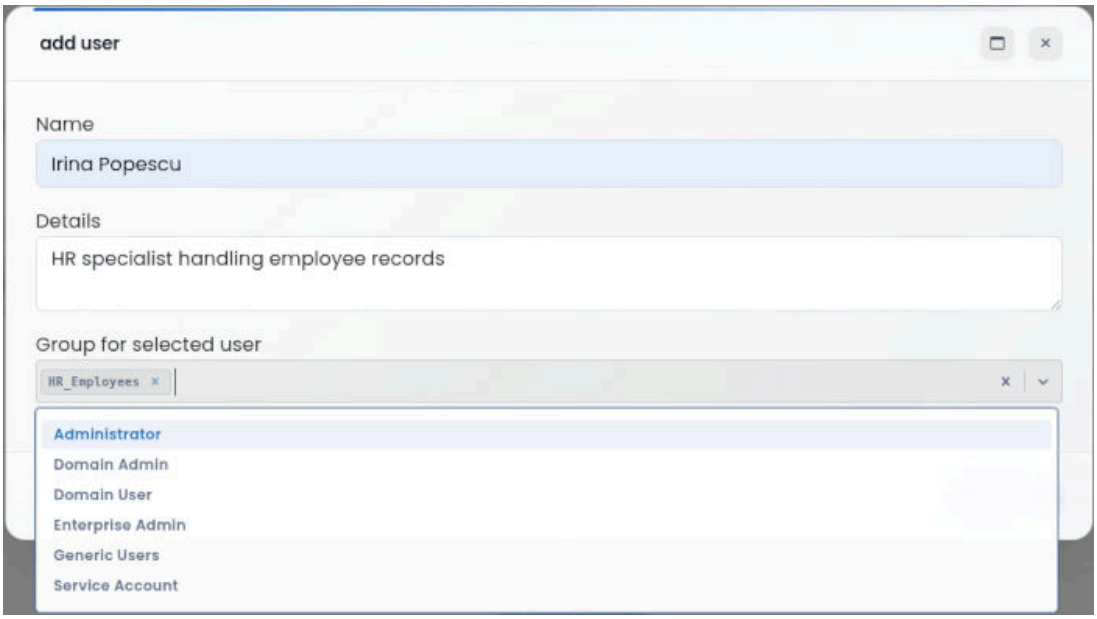


Users

Assign users to UEBA user groups.



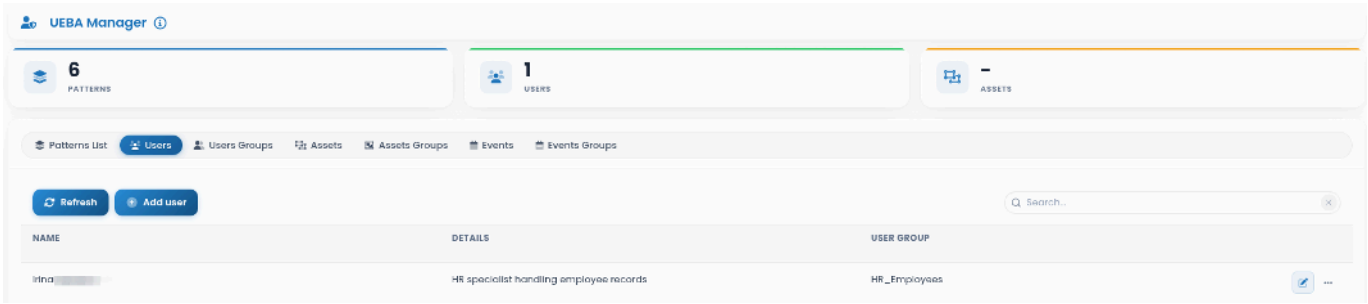
To add a user, click the "***Add User***" button.



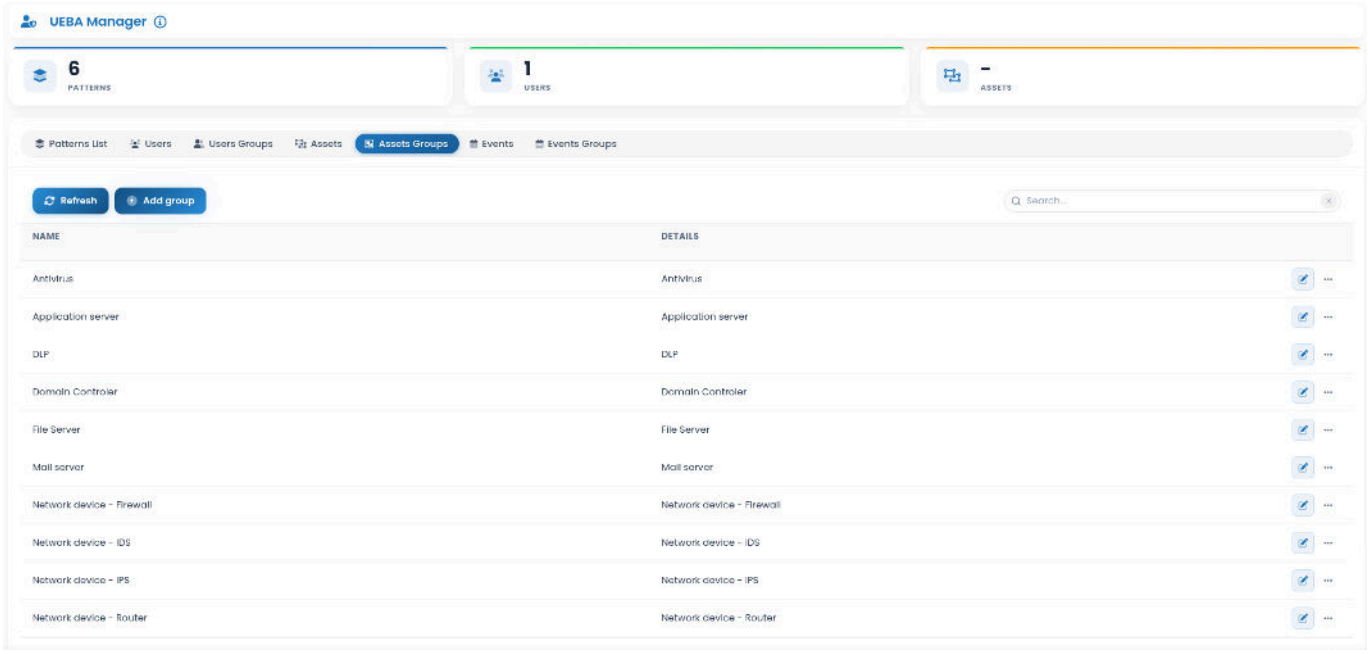
- **Name:** Name that identifies the user
- **Details:** Additional details about the user
- **Group for selected user:** Group to which the user belongs

Click **Save** to create or update the user entry, or **Cancel** to discard.

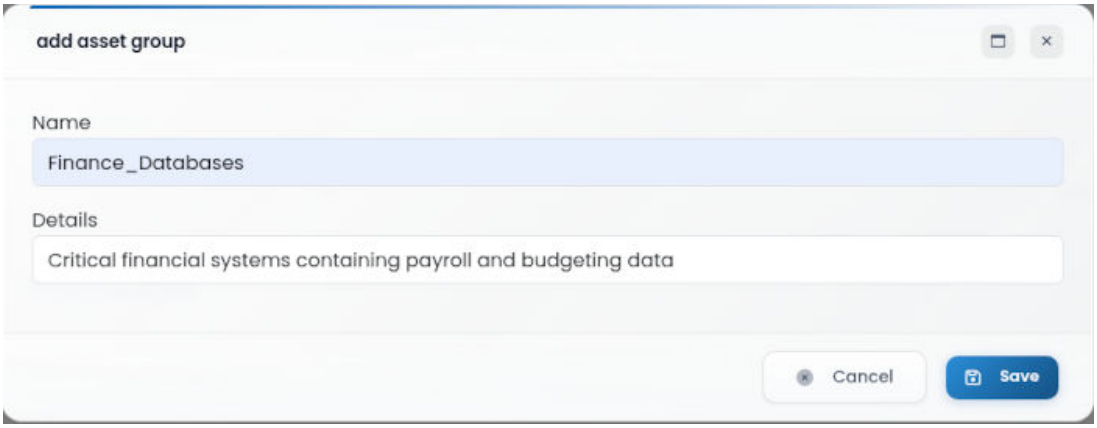
The **Users** view lists configured users and provides options to edit, update, or delete:



Asset groups



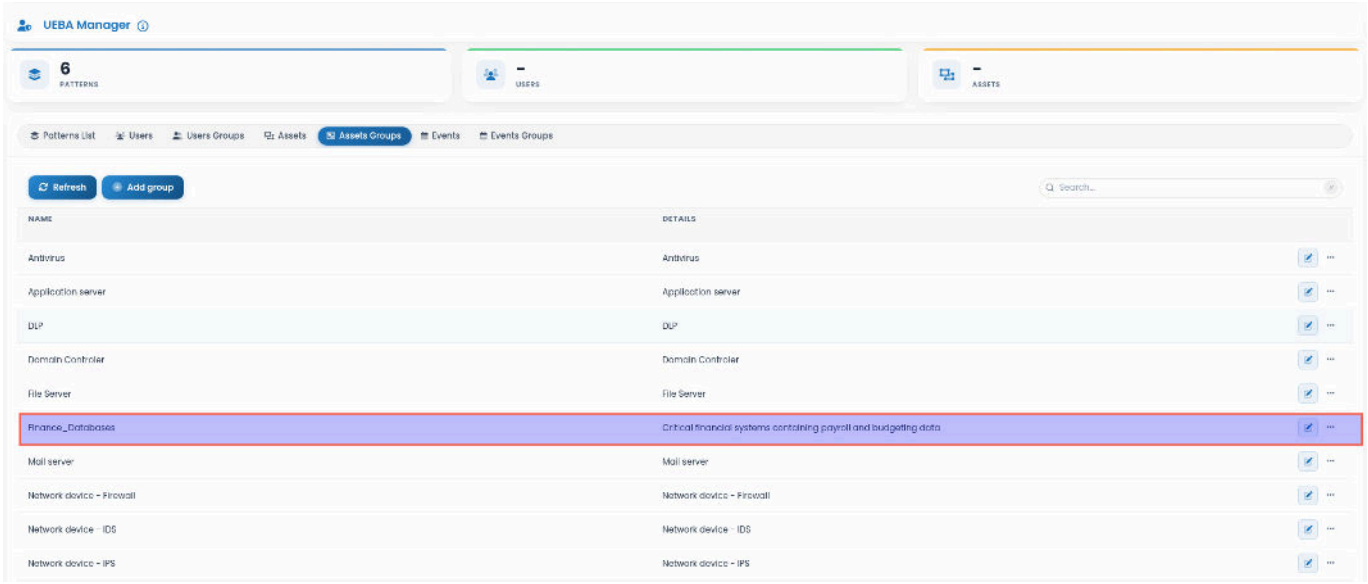
Create a group in **Assets Groups** by clicking the add button:



- **Name:** Name that identifies the asset group
- **Details:** Additional details about the group

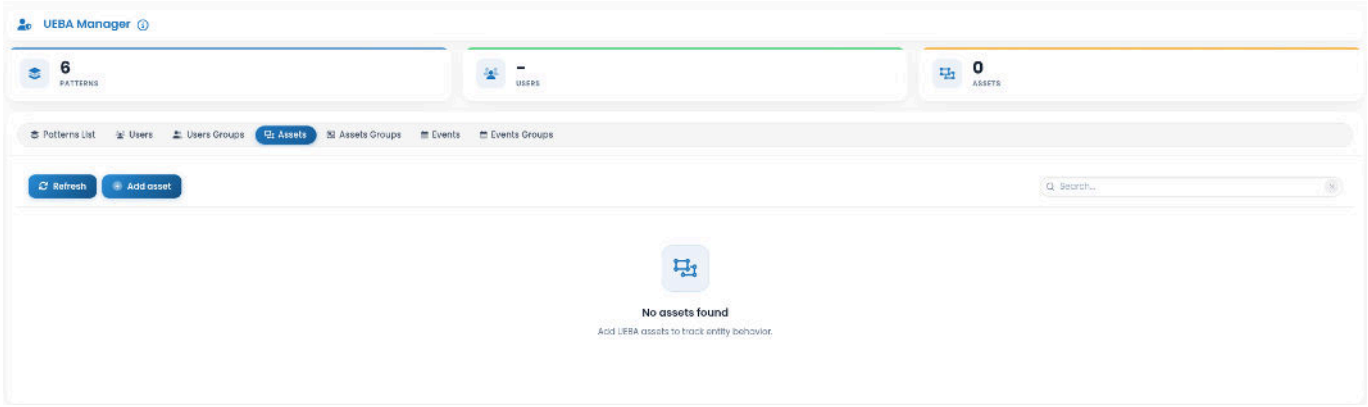
Click **Save** to create the asset group, or **Cancel** to discard.

The **Assets Groups** view lists existing groups and provides options to edit, update, or delete:

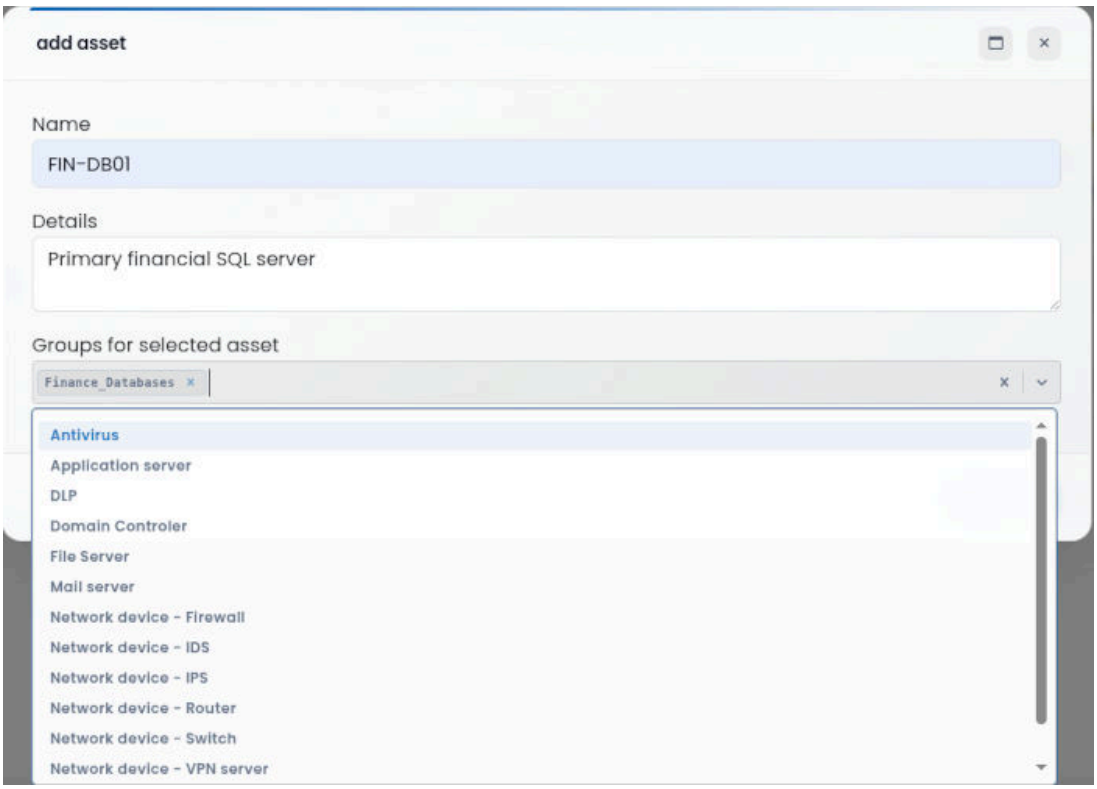


Assets

Assign assets to UEBA asset groups.



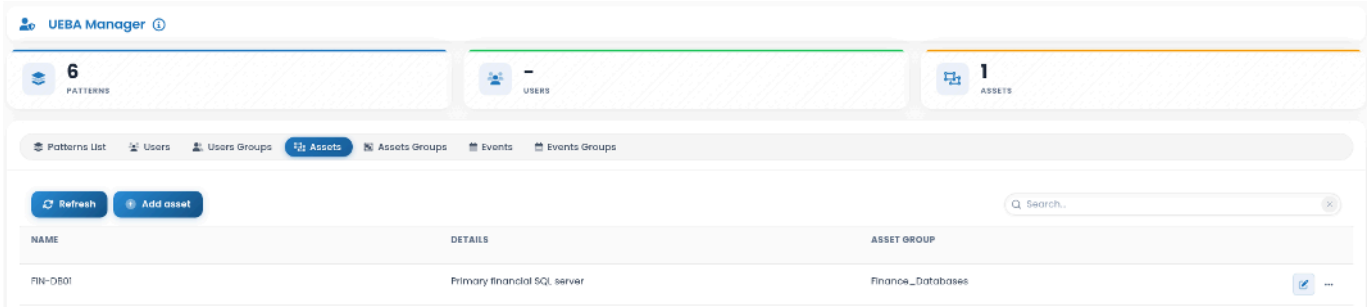
To add an asset, click the "***Add asset***" button:



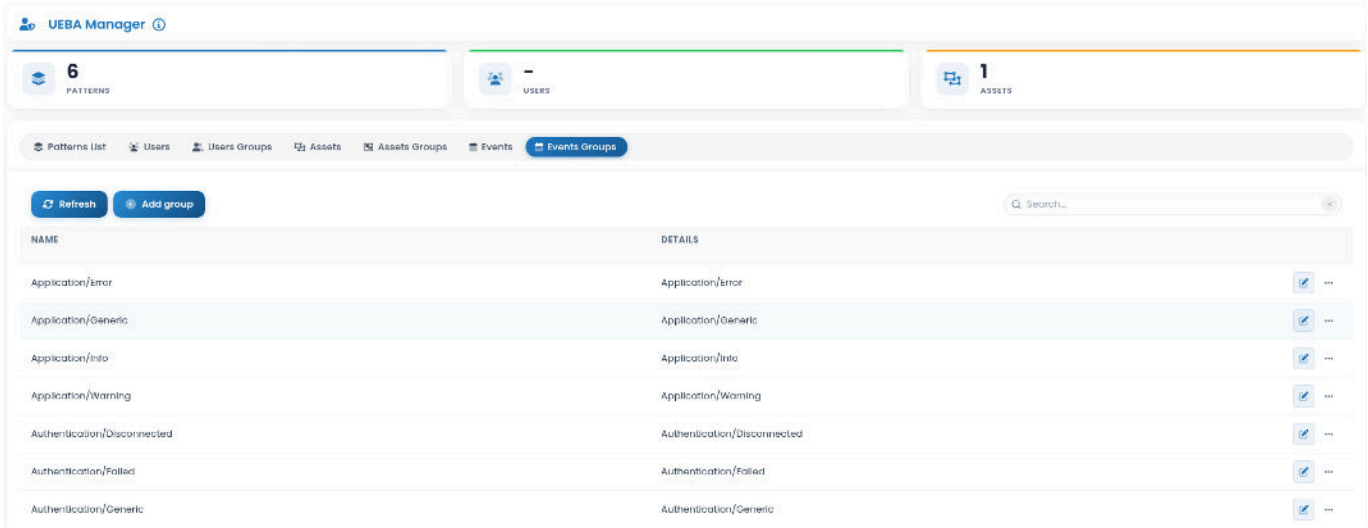
- **Name:** Name that identifies the asset
- **Details:** Additional details about the asset
- **Group for selected asset:** Group to which the asset belongs

Click **Save** to create or update the asset entry, or **Cancel** to discard.

The **Assets** view lists configured assets and provides options to edit, update, or delete:



Event groups



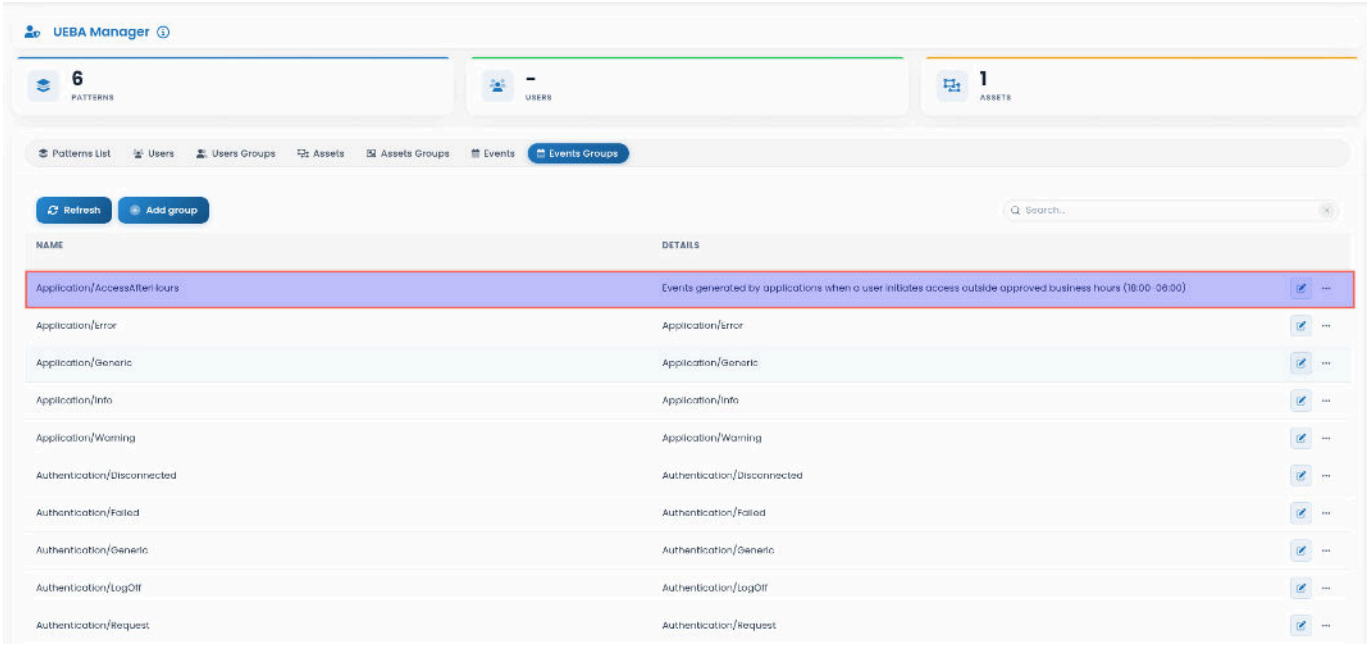
Create a group in **Events Groups** by clicking the add button:



- **Name:** Name that identifies the event group
- **Details:** Additional details about the group

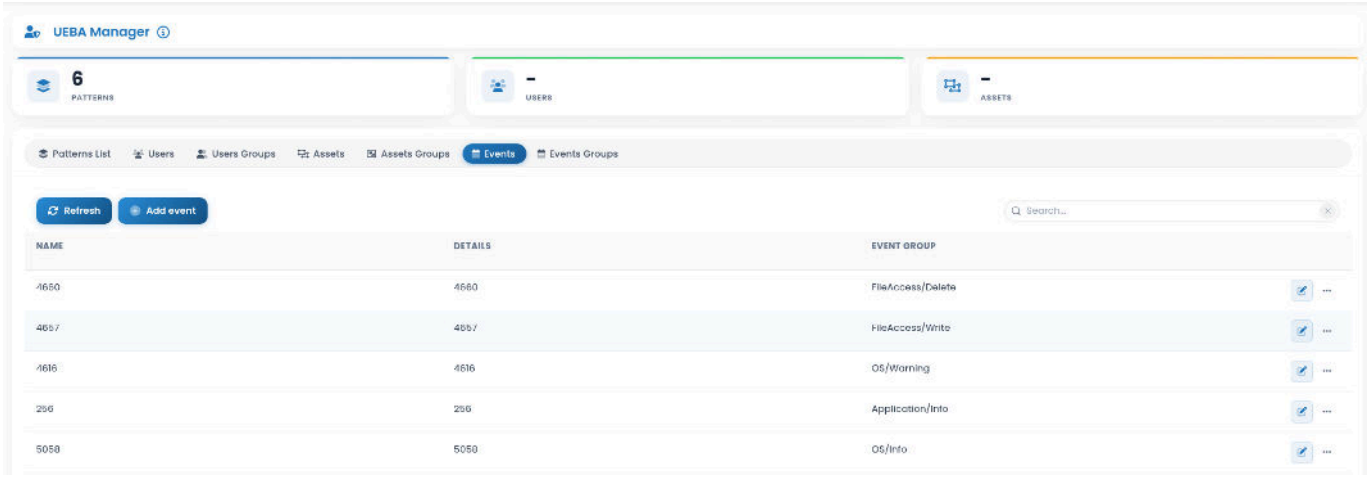
Click **Save** to create the event group, or **Cancel** to discard.

The **Events Groups** view lists existing groups and provides options to edit, update, or delete:

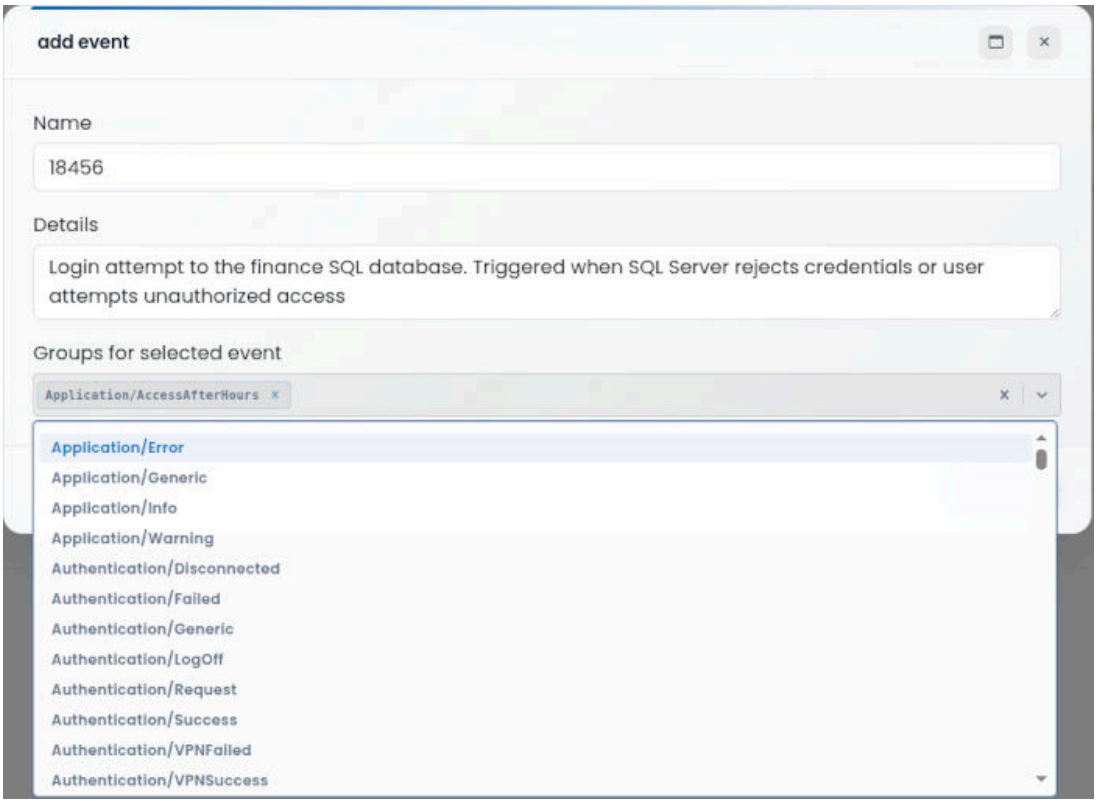


Events

Assign events to UEBA event groups.



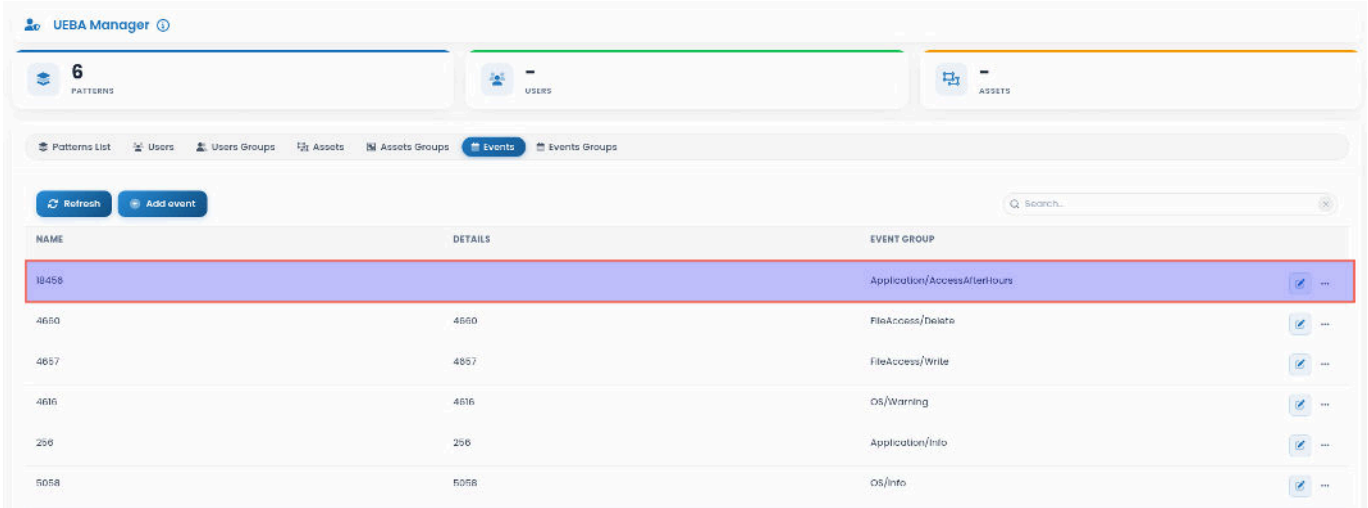
To add an event, click the "***Add event***" button:



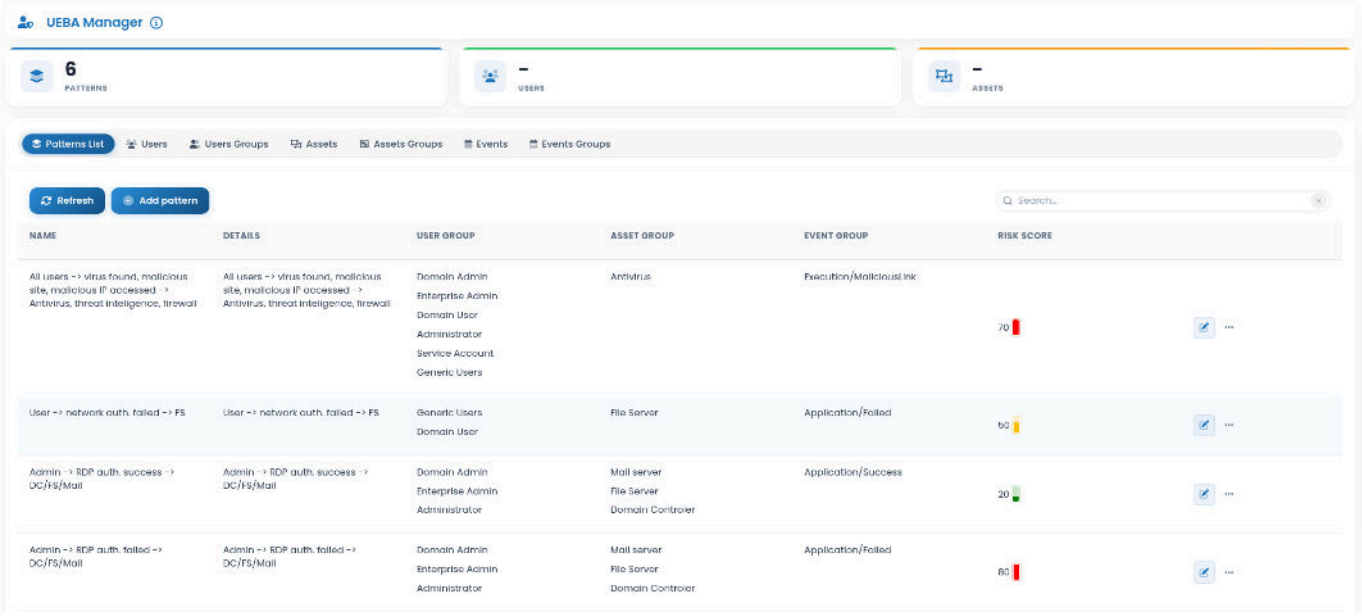
- **Name:** Name that identifies the event
- **Details:** Additional details about the event
- **Group for selected event:** Group to which the event belongs

Click **Save** to create or update the event entry, or **Cancel** to discard.

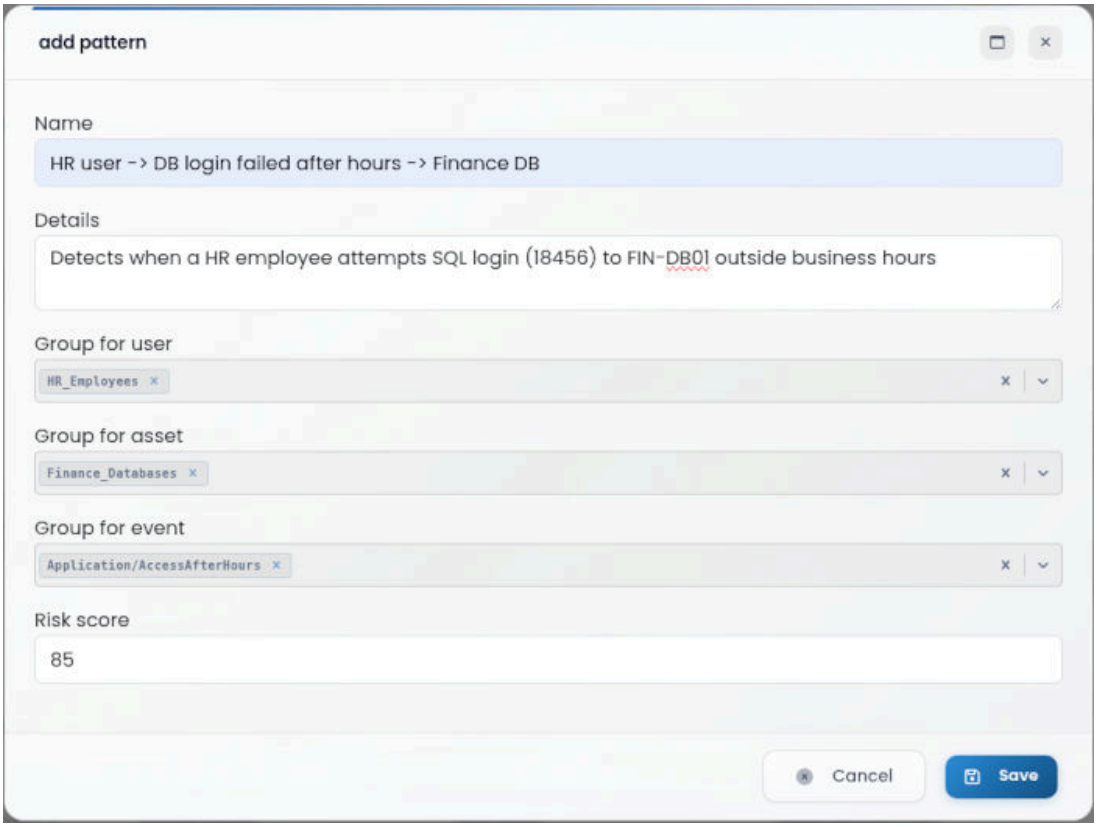
The **Events** view lists configured events and provides options to edit, update, or delete:



Patterns list

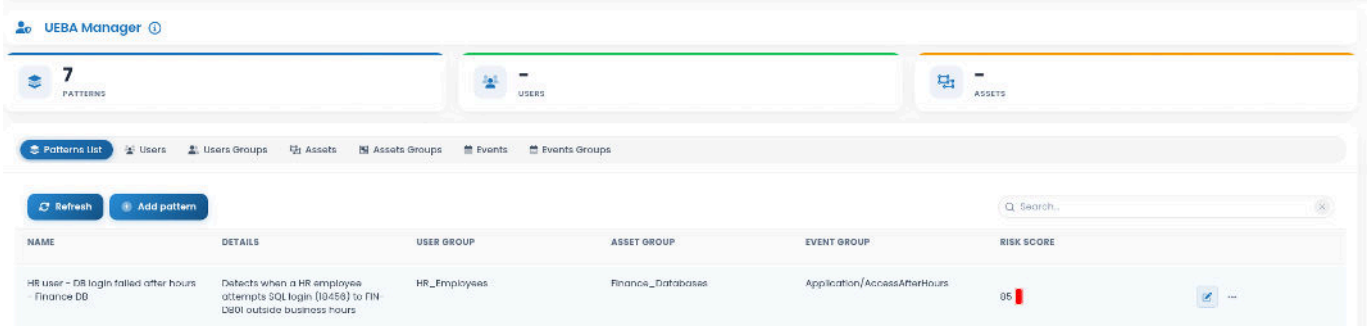


Define patterns that determine the risk factor associated with each event. To add a pattern, click the "***Add pattern***".



- **Name:** Name that identifies the pattern
- **Details:** Additional details about the pattern
- **Group for user:** User group to which the pattern applies (from Users Groups)
- **Group for asset:** Asset group to which the pattern applies (from Assets Groups)
- **Group for event:** Event group to which the pattern applies (from Events Groups)
- **Risk score:** Risk score from 0 to 100 associated with the pattern

The **Patterns** view lists configured patterns and provides options to edit, update, or delete:



Operations · How to manually deploy agent and assign data sources

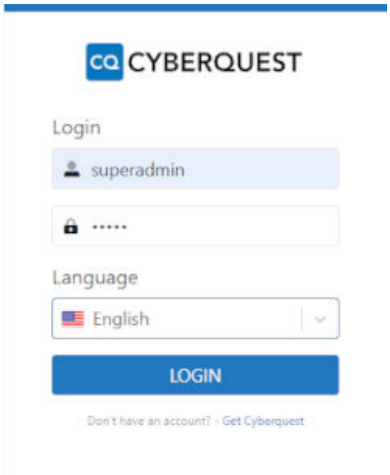
Prerequisites

Before installing the CYBERQUEST agent on a Windows target machine, ensure the following components are installed:

1. vcredist_x64_2010.exe (https://www.microsoft.com/en-us/download/confirmation.aspx?id=26999)
2. vcredist_x64_2012.exe (https://www.microsoft.com/en-us/download/confirmation.aspx?id=30679)
3. vc_redist_x64_2019.exe (https://aka.ms/vs/16/release/vc_redist.x64.exe)
4. Microsoft .NET Framework 4.8 (https://go.microsoft.com/fwlink/?linkid=2088631)

Authentication

To access the web interface, open a browser and enter the application's IP address or DNS name (for example, ***https://CyberquestIPAddress***). The browser redirects to the CYBERQUEST authentication page:



Credentials

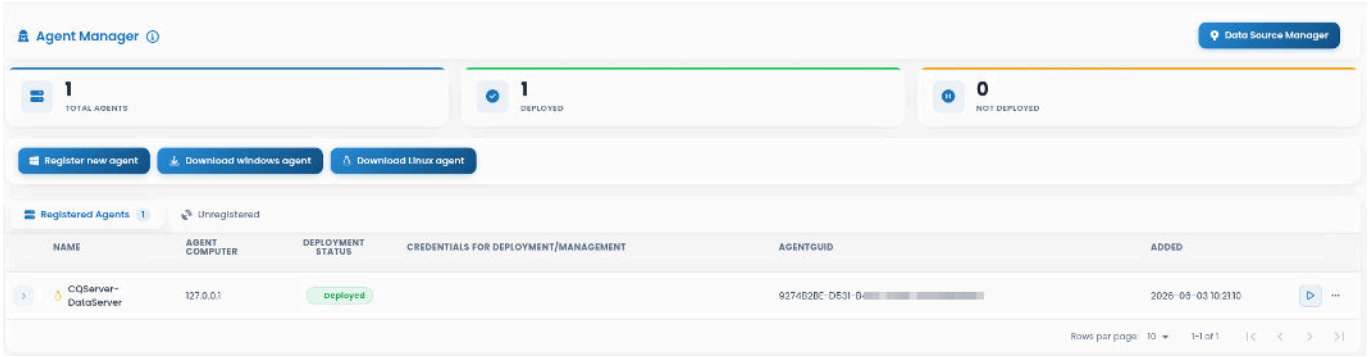
Credentials define the accounts agents use when collecting data. See How to manage credentials for details on creating and maintaining credential entries.

Installing the CYBERQUEST agent

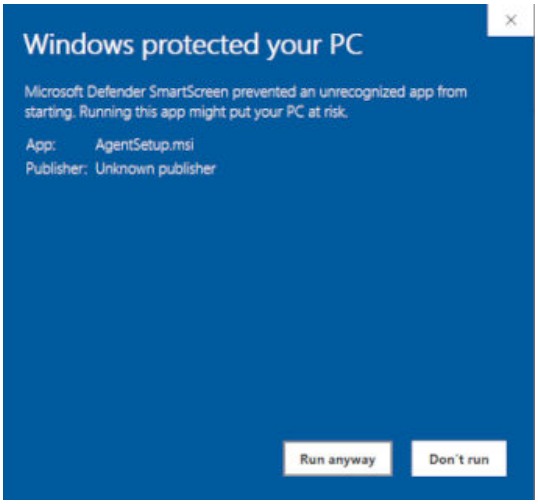
To manually deploy the agent, download or copy the agent kit to the target Windows machine.

Navigate to **Settings > Management > Agent Manager**.

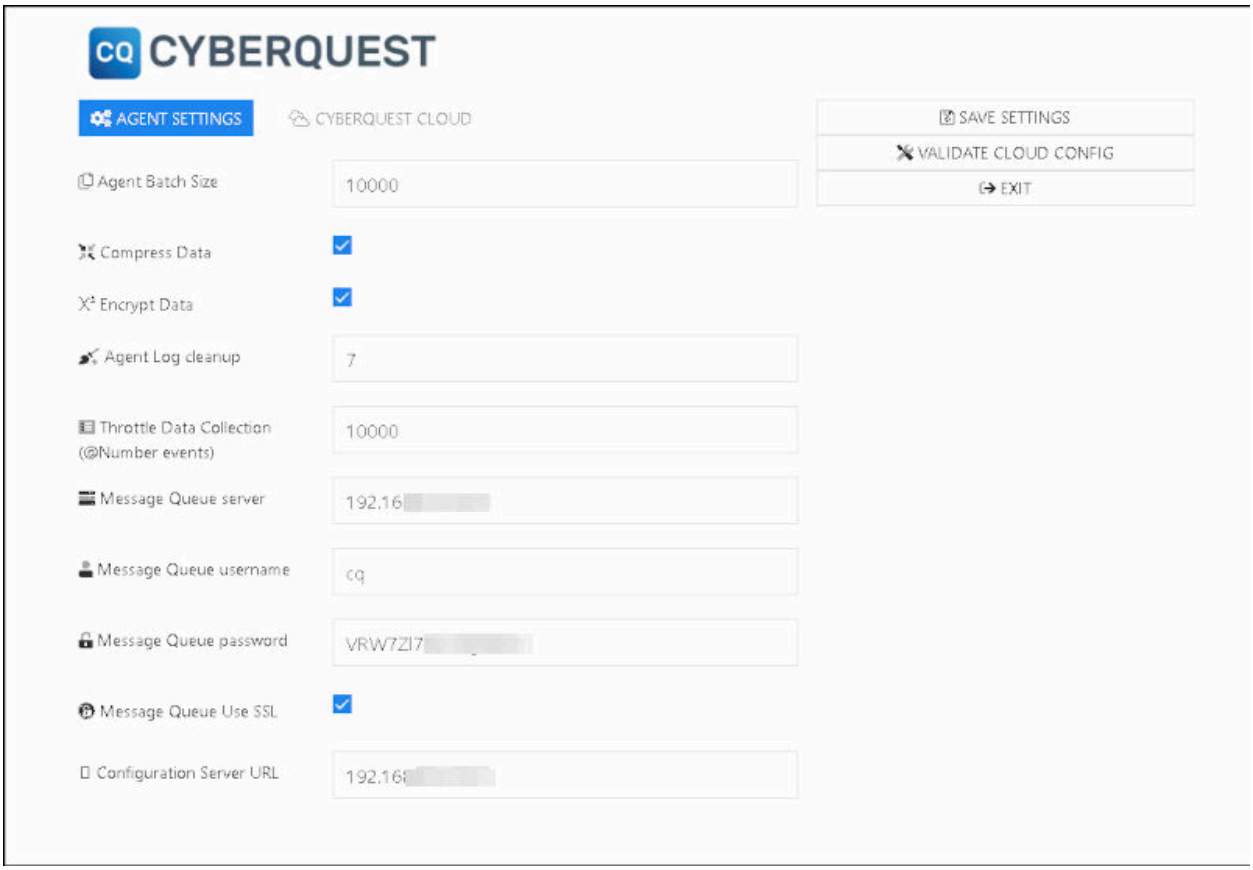
Use **Download Windows agent** to download the latest version of the CYBERQUEST agent.



Run the `.msi` installer. If prompted with a security warning, choose **Run anyway** to continue. The agent is installed to `C:\Program Files\CyberQuestAgent`.



Open `C:\Program Files\CyberQuestAgent\configurator` and run **cyberquest-agent-configurator.exe** as an Administrator. In **Message Queue server**, enter the CYBERQUEST server IP address and click **Save Settings**.



In Windows Services, restart the CYBERQUEST Agent service.

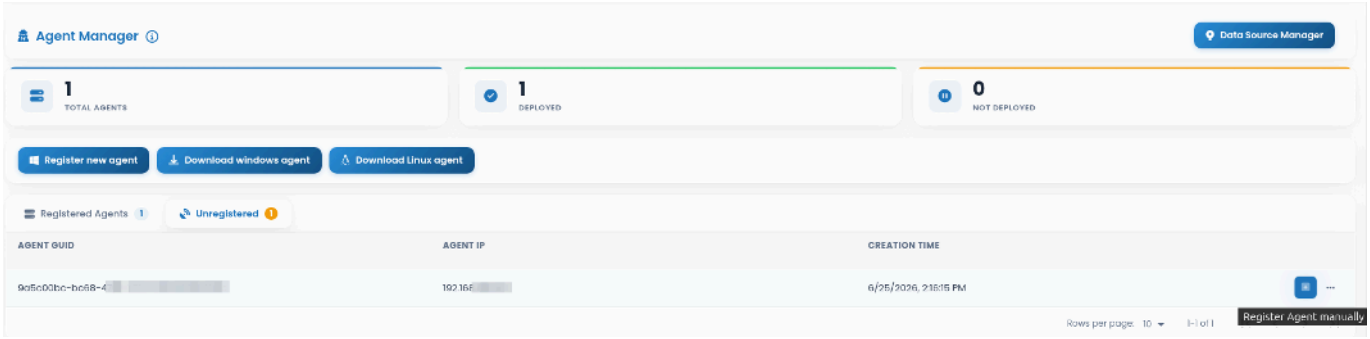
Registering the agent

Register the agent in the CYBERQUEST server from **Settings > Management > Agent Manager**.

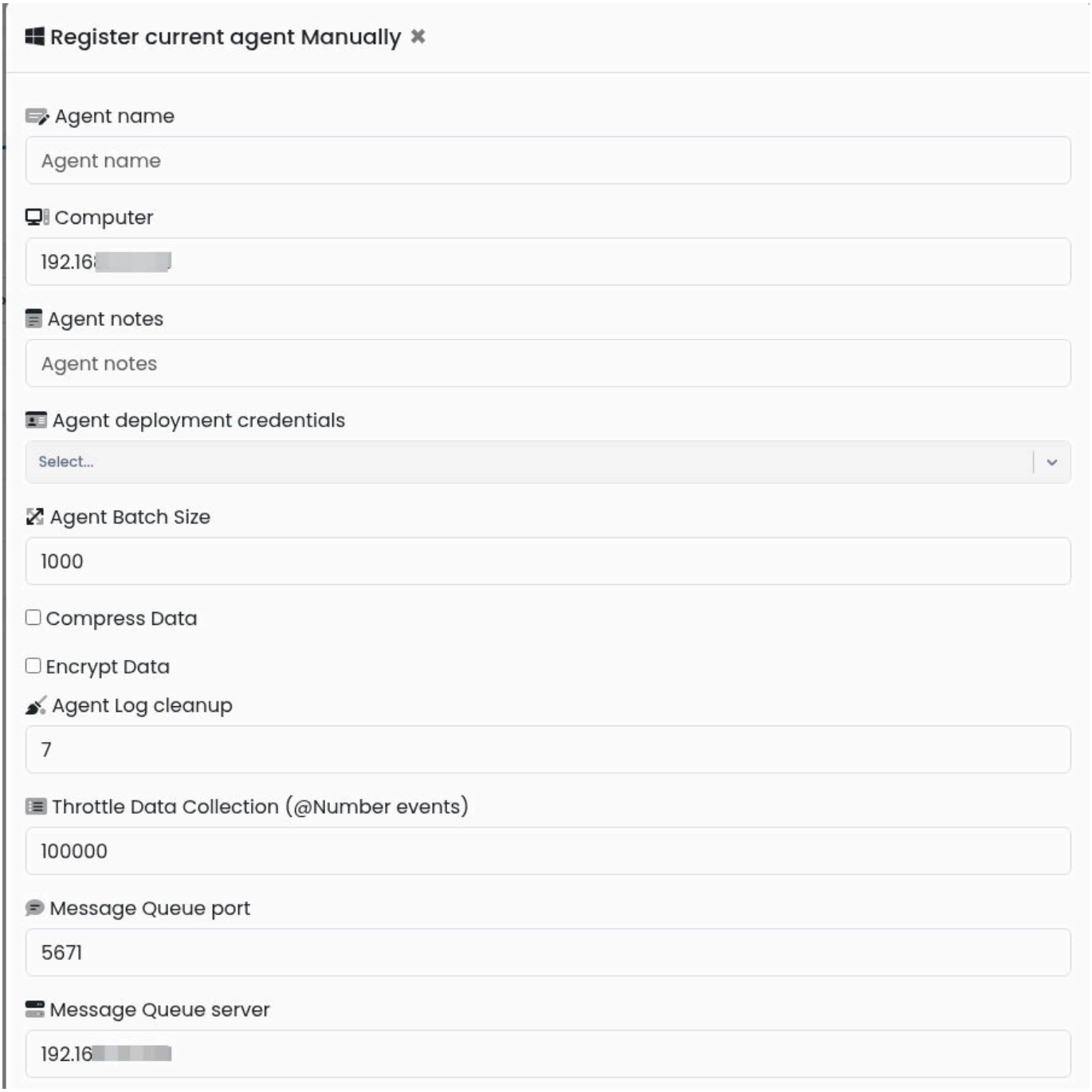
Go to ***Unregistered*** page and press

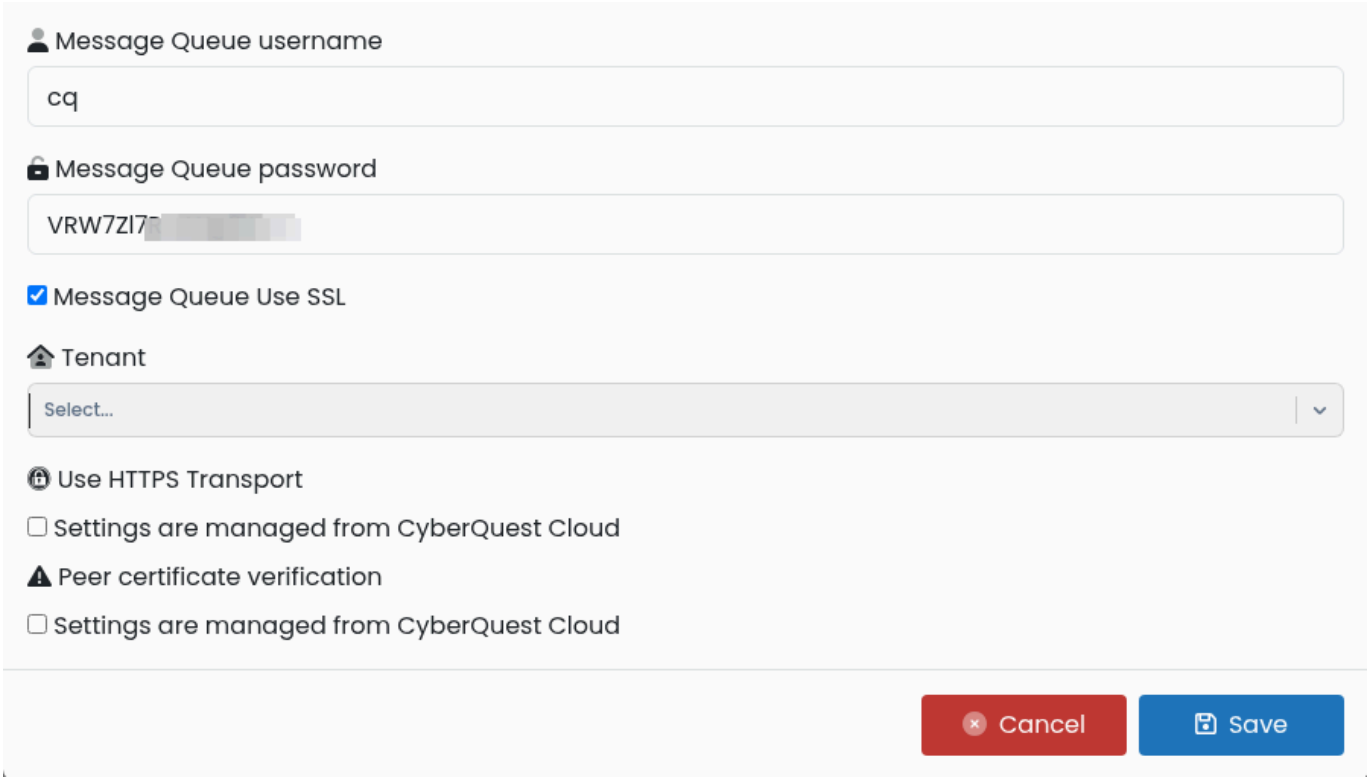


button to register the agent.



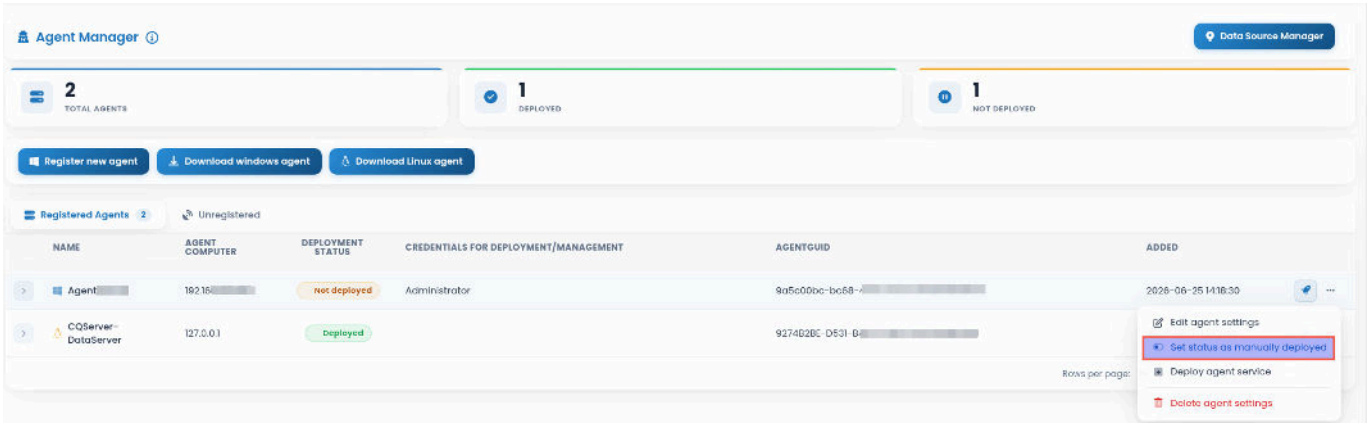
Complete the fields **Agent name**, **Agent note**, and assign credentials for the agent, then click **Save**.


Register current agent Manually
Agent name
Agent name
Computer
192.16
Agent notes
Agent notes
Agent deployment credentials
Select...
Agent Batch Size
1000
Compress Data
Encrypt Data
Agent Log cleanup
7
Throttle Data Collection (@Number events)
100000
Message Queue port
5671
Message Queue server
192.16



After deployment, navigate to **Registered Agent** and click the **Set status as manually deployed**

button:



Adding new data sources

The Windows agent connects to and collects data from the following data sources:

- WMI (Windows Management Instrumentation):
  - Windows Security Log
  - Windows Application Log
  - Windows System Log
  - Active Directory Information
- CQ Threat Intelligence
- ODBC data sources
- Oracle-based data sources
- MySQL (MariaDB)–based data sources

- API-based data sources
- Text files (free text and CSV)

Operations · How to manually deploy agent for Windows based collections

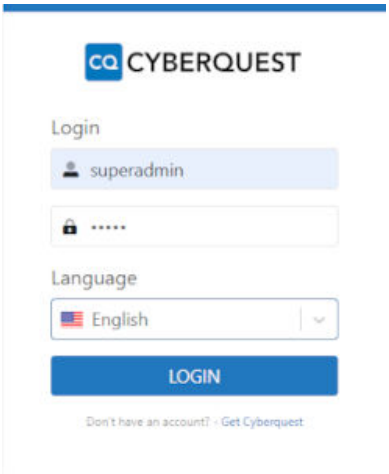
Prerequisites

Before installing the CYBERQUEST agent on a Windows target machine, ensure the following components are installed:

1. vcredist_x64_2010.exe (https://www.microsoft.com/en-us/download/confirmation.aspx?id=26999)
2. vcredist_x64_2012.exe (https://www.microsoft.com/en-us/download/confirmation.aspx?id=30679)
3. vc_redist_x64_2019.exe (https://aka.ms/vs/16/release/vc_redist.x64.exe)
4. Microsoft .NET Framework 4.8 (https://go.microsoft.com/fwlink/?linkid=2088631)

Authentication

To access the web interface, open a browser and enter the application's IP address or DNS name (for example, ***https://CyberquestIPAddress***). The browser redirects to the CYBERQUEST authentication page:



Credentials

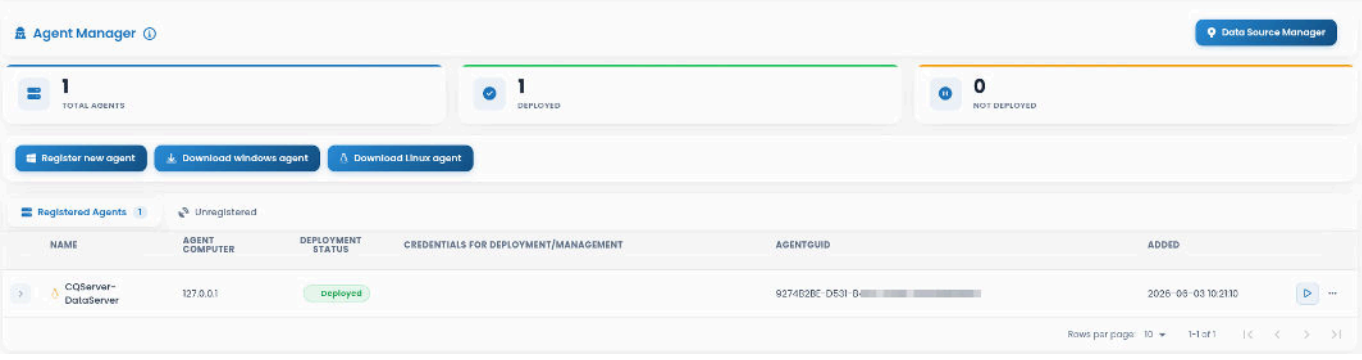
Credentials define the accounts agents use when collecting data. See How to manage credentials for details on creating and maintaining credential entries.

Installing the CYBERQUEST agent

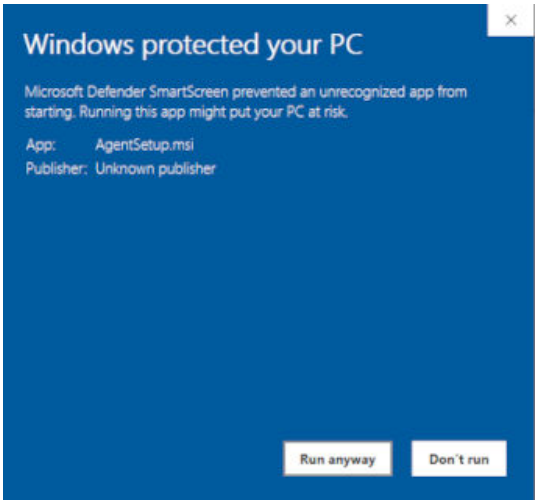
To manually deploy the agent, download or copy the agent kit to the target Windows machine.

Navigate to **Settings > Management > Agent Manager**.

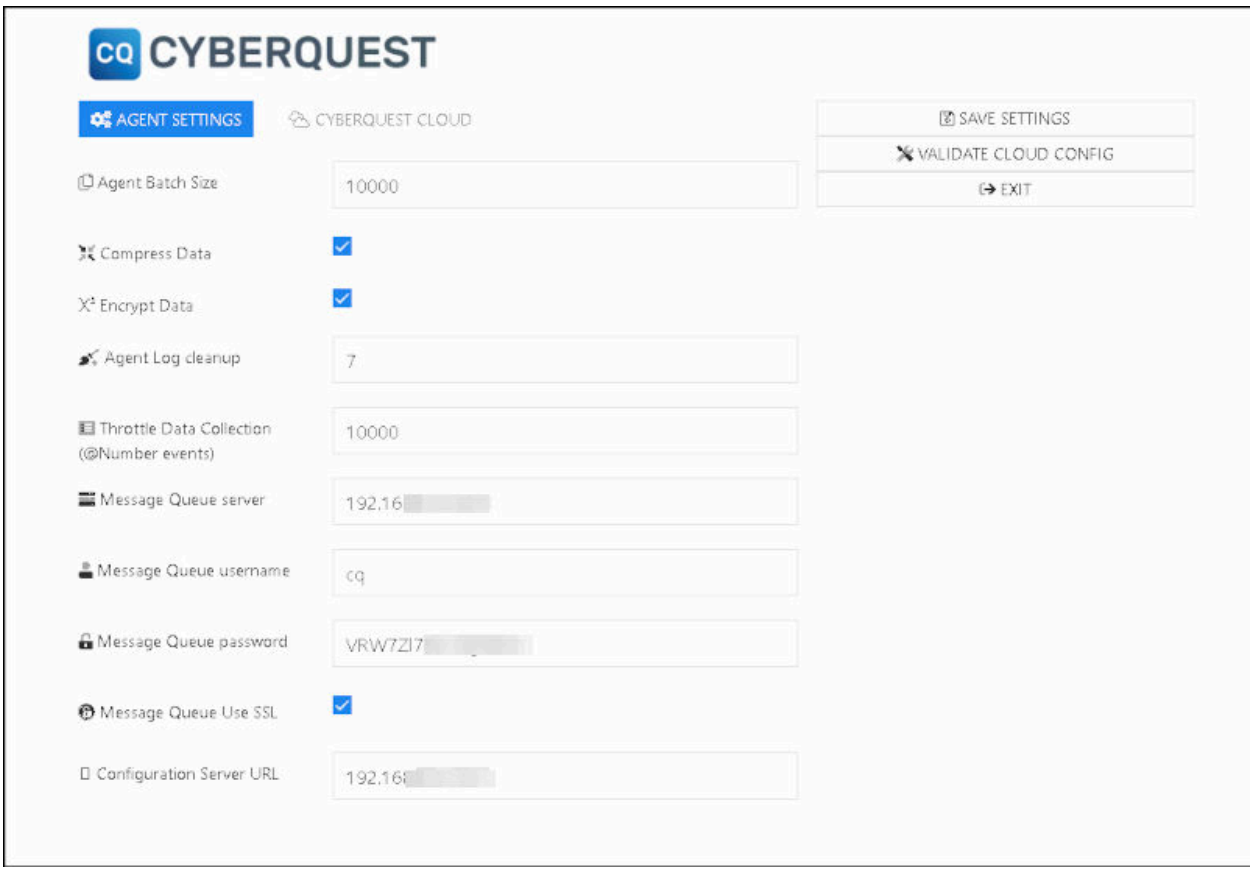
Use **Download Windows agent** to retrieve the latest version of the CYBERQUEST agent.



Run the `.msi` installer. If prompted with a security warning, choose **Run anyway** to continue. The agent is installed to `C:\Program Files\CyberQuestAgent`.



Open `C:\Program Files\CyberQuestAgent\configurator` and run **cyberquest-agent-configurator.exe** as an Administrator. In **Message Queue server**, enter the CYBERQUEST server IP address and click **Save Settings**.



In Windows Services, restart the CYBERQUEST Agent service.

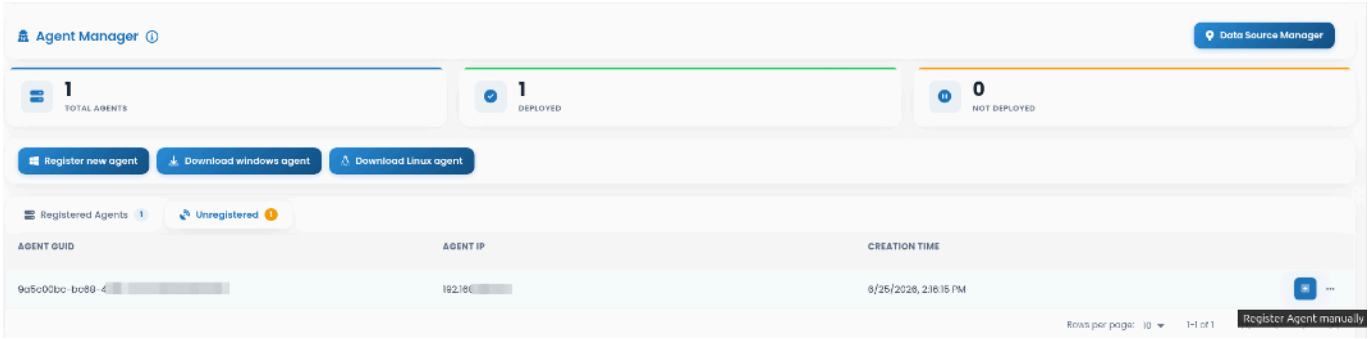
Registering the agent

Register the agent in the CYBERQUEST server from **Settings > Management > Agent Manager**.

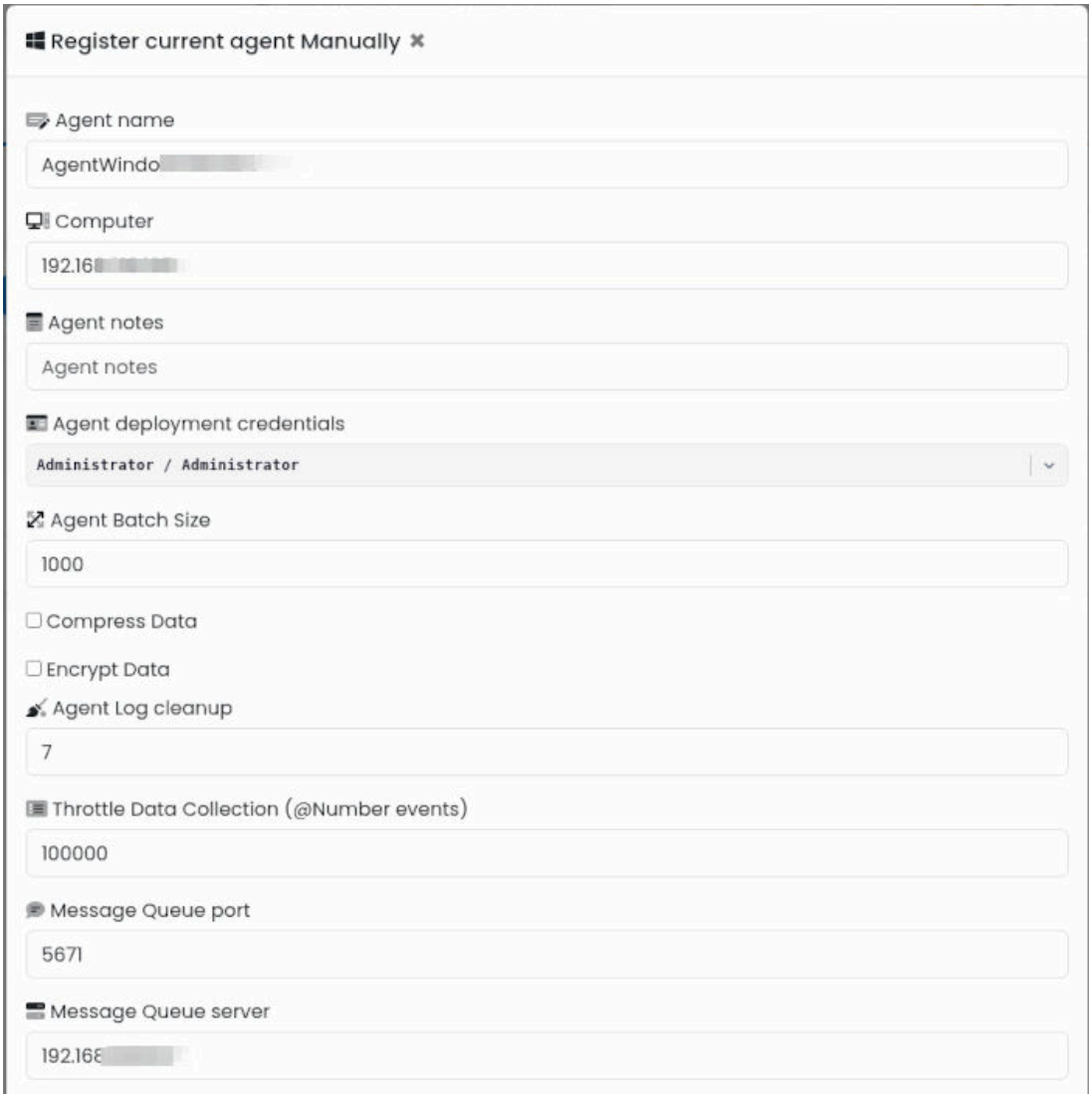
Go to ***Unregistered*** page and press

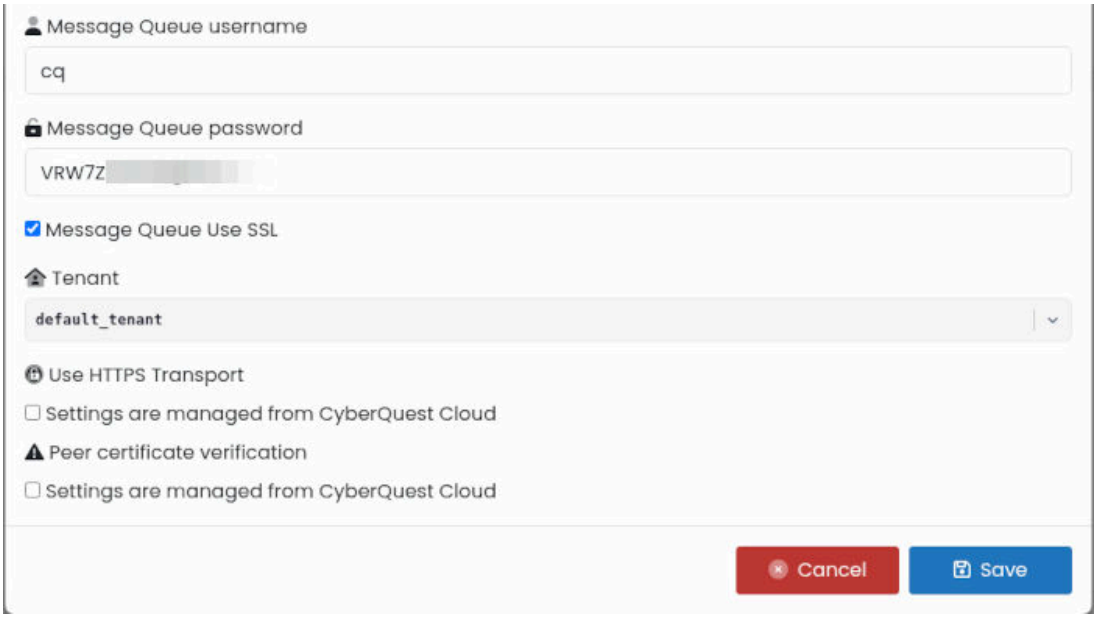


button to register the agent.



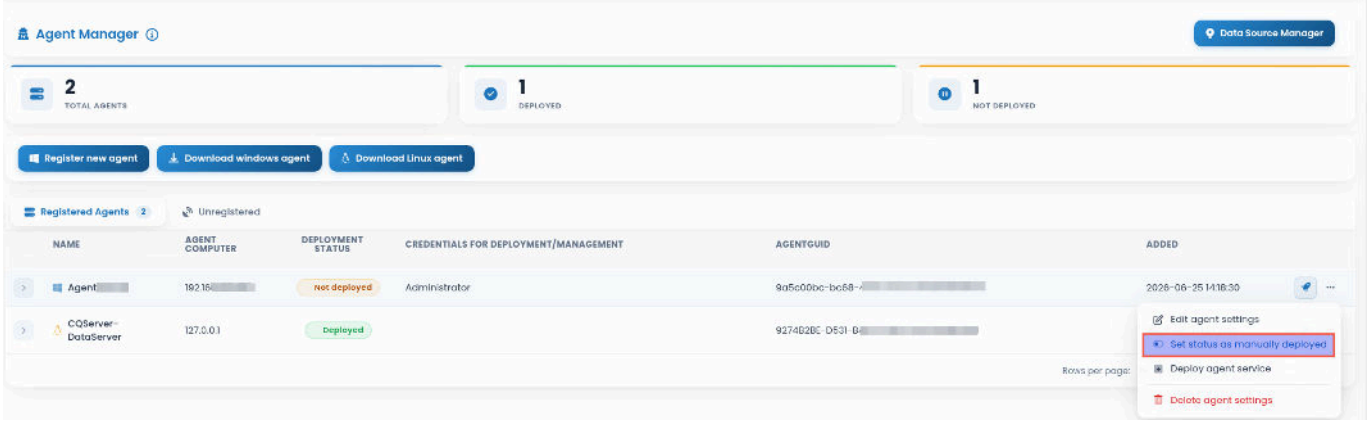
Complete **Agent name**, **Agent note**, and assign credentials for the agent, then click **Save**.





After deployment, navigate to **Registered Agent** and click the **Set status as manually deployed**

button:



Operations · How to monitor administrative privileges use

Monitoring administrative privileges requires configuring audit coverage, building views, and scheduling reports.

1. Ensure audit data is collected

Collect operating system and application logs that record privileged actions:

- Windows: security, system, and Active Directory audit logs (for example, account management, logon/logoff, policy changes)
- Linux: system logs for user/group creation, privilege elevation, and sudo activity

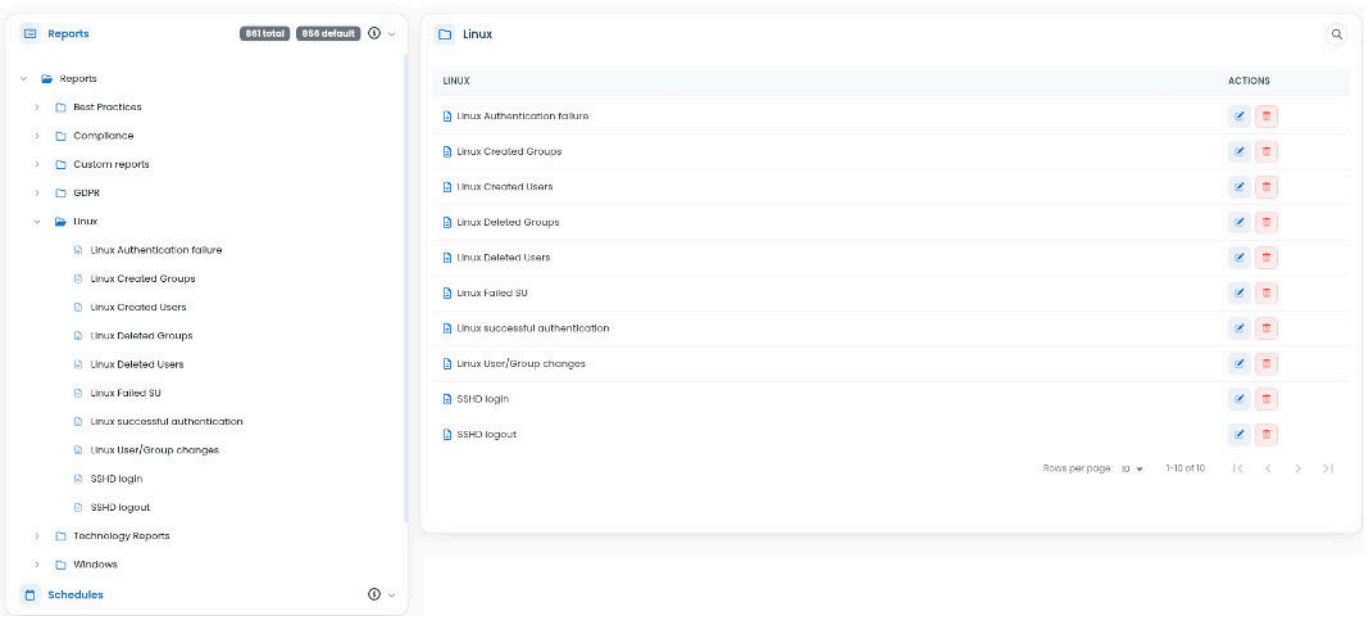
Relevant collection guides include:

- How to collect data on Windows Security Log
- How to collect data on Windows System Log
- How to collect data on Active Directory

2. Define which privileged actions are relevant

Focus on high-risk actions:

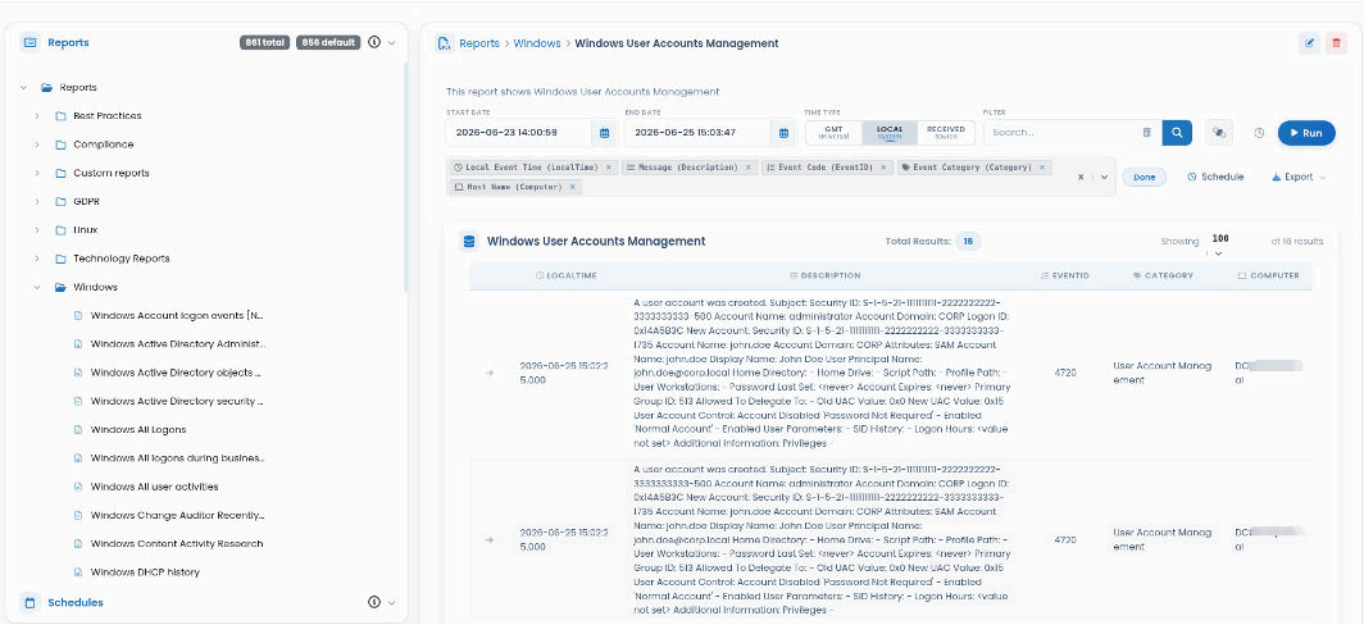
- Windows: user creation, event log cleared, password resets, user account management
- Linux: group creation, user creation, user/group deletion



Additional guidance for self-audit of CYBERQUEST users is available in: How to monitor CYBERQUEST user activities.

3. Use reports to review activity

Run reports interactively for investigations or schedule them for regular delivery (for example, daily or weekly summaries of administrative changes).



For details on creating and running reports, see: How to create a new report and run it.

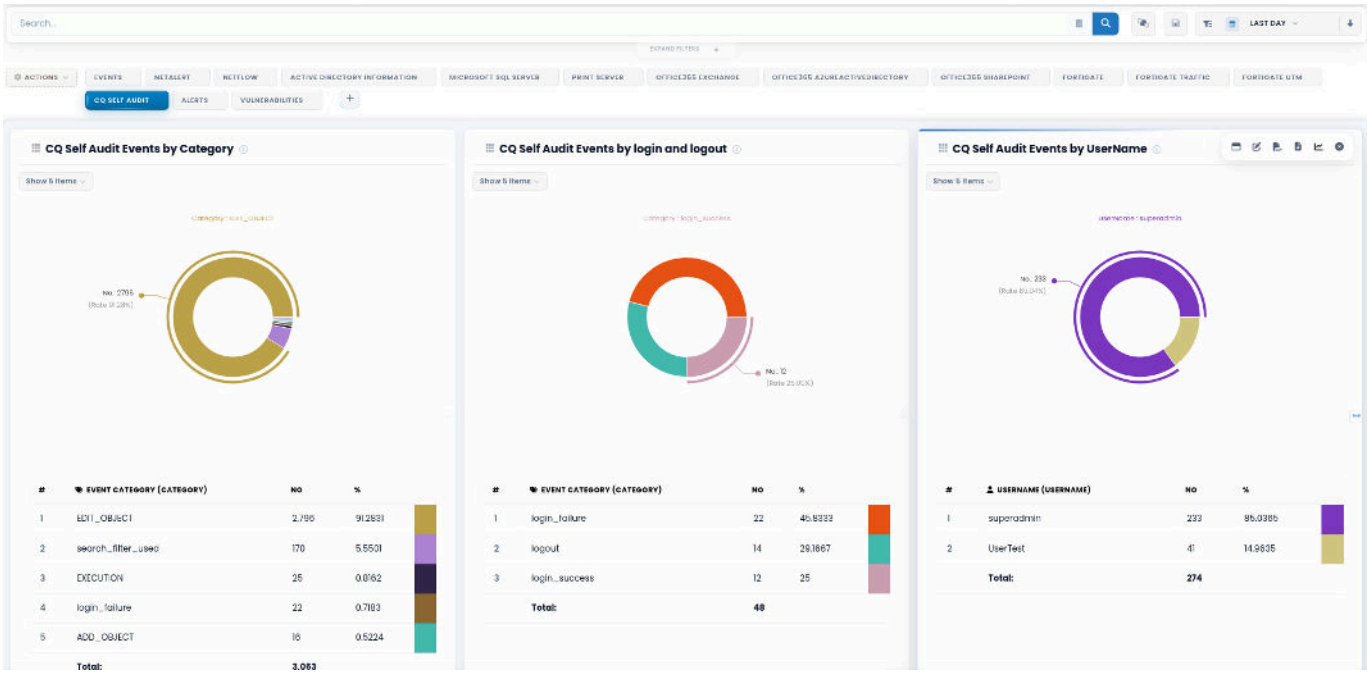
Operations · How to monitor cyberquest user activities

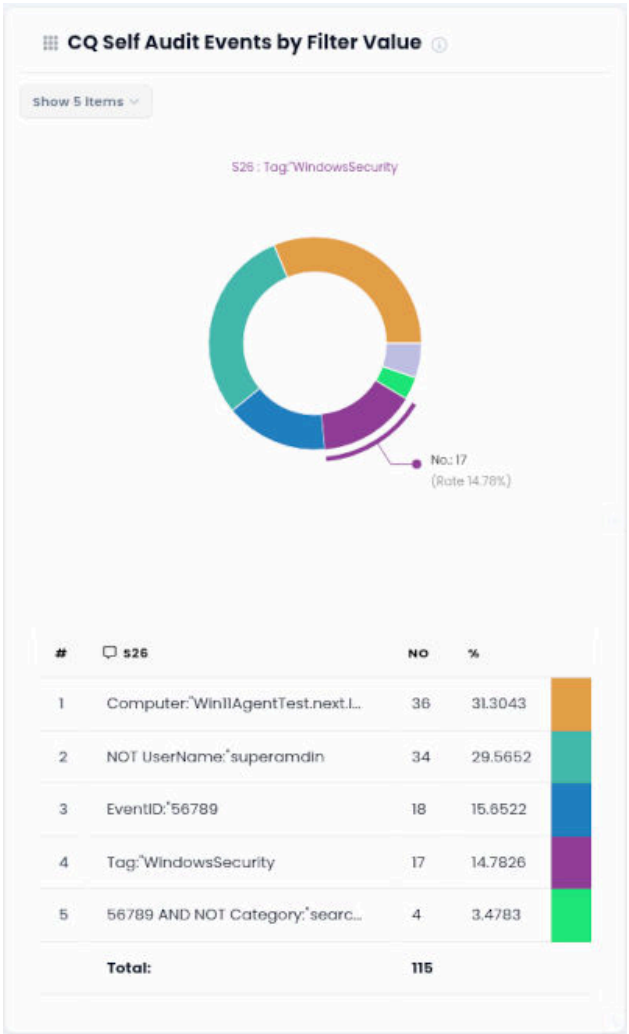
CYBERQUEST includes self-audit capabilities. All Web interface activities are automatically logged under

```
EventID:56789
```

Also, operating system auditing is enabled by default and information is automatically collected.

Dashboards can also be added to quickly display CQ Users activity. The preset is called “CQ Self Audit” and be added in dashboards module.





Operations · How to monitor inactive accounts

Monitoring inactive accounts combines object lists, alert correlation, and reporting.

1. Creating Object List Entries

Follow the steps below to add each inactive account into the **Inactive_accounts** Object List.

1.1 Access the Object Management Module

- Log in to CYBERQUEST with an account that has administrative or configuration permissions.
- Navigate to the menu: **Settings > Management > Objects**

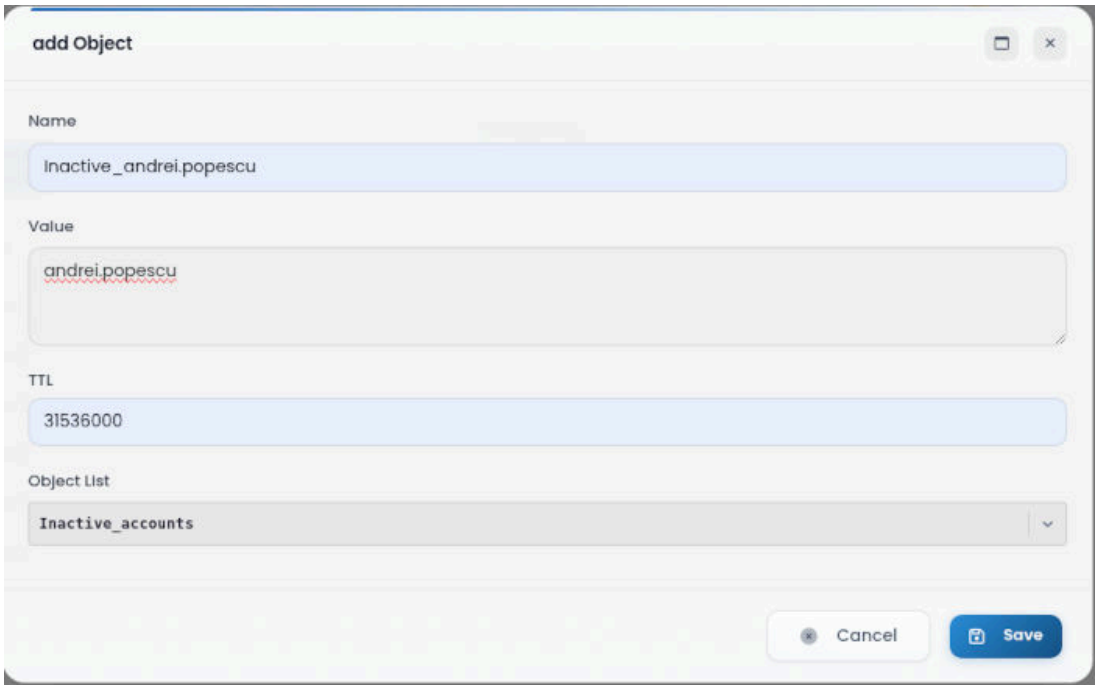
1.2 Create a New Object Entry

Follow the steps below to add an inactive account into the **Inactive_accounts** Object List:

In the **Objects** page, click **NEW OBJECT**.

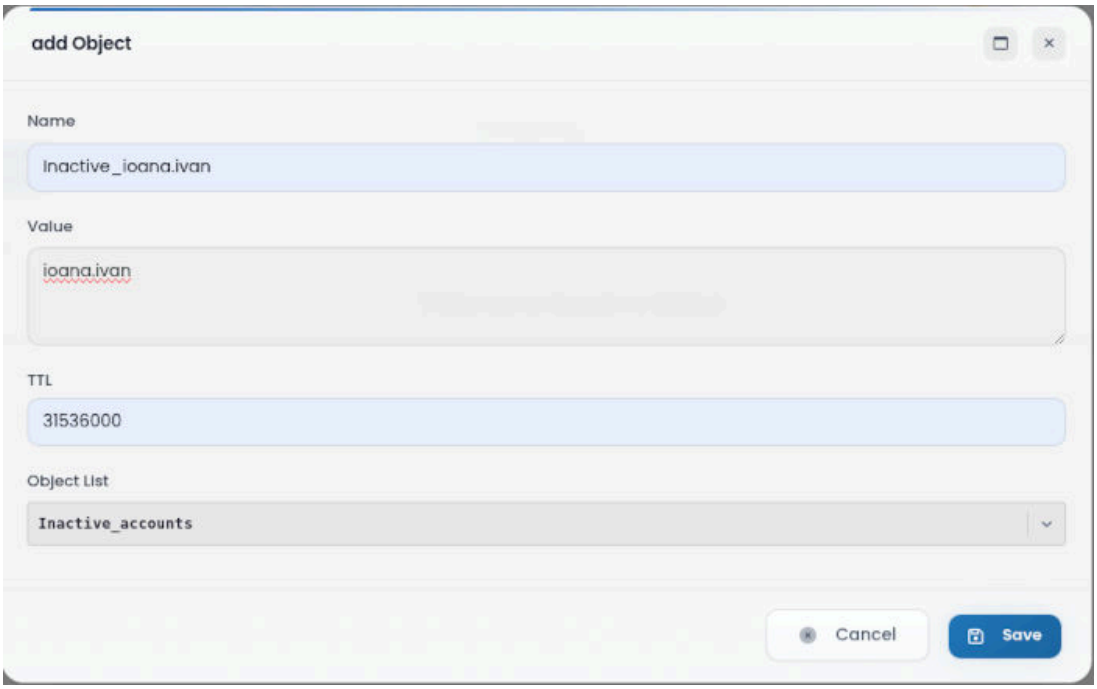
- In the **Name** field, enter a clear identifier for the inactive account.
- In the **Value** field, enter the exact username as it appears in event logs.
- **Set TTL = 1 Year** - TTL must be specified in seconds.
- **Assign to Object List** - In the **Object List** field, select: **Inactive_accounts**

  If the list does not exist, type the name and choose **Create "Inactive_accounts"**

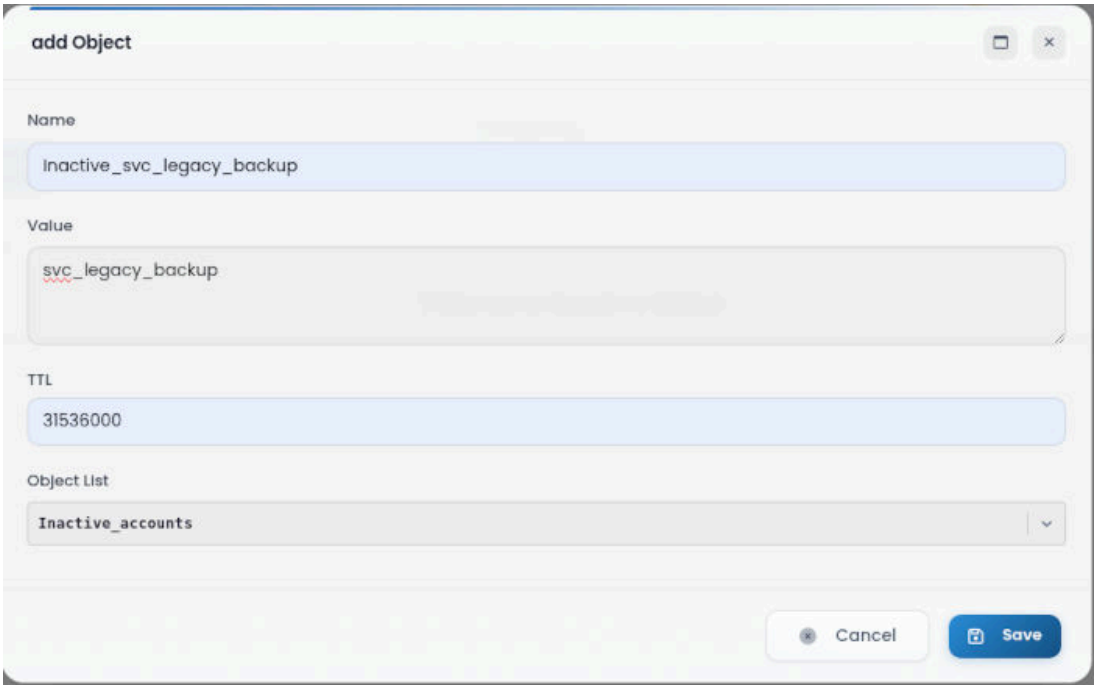


- Click **Save** to store the entry.

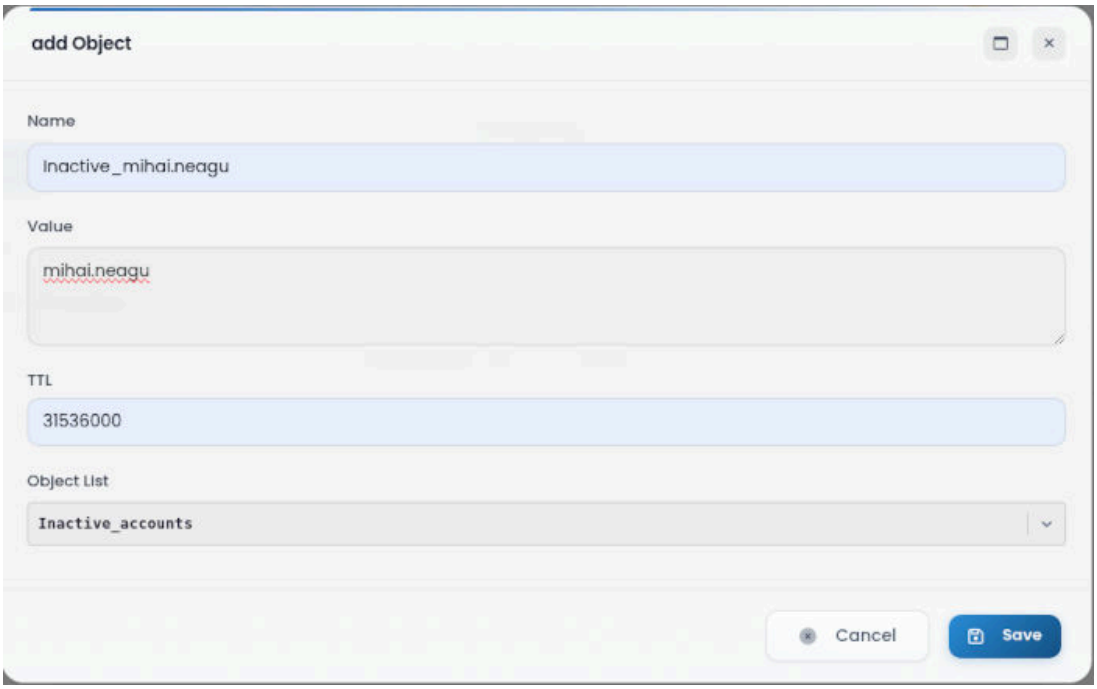
Repeat the steps in section 2.2 to create additional object entries for:



Repeat the steps in section 2.2 to create additional object entries for:



Repeat the steps in section 2.2 to create additional object entries for:

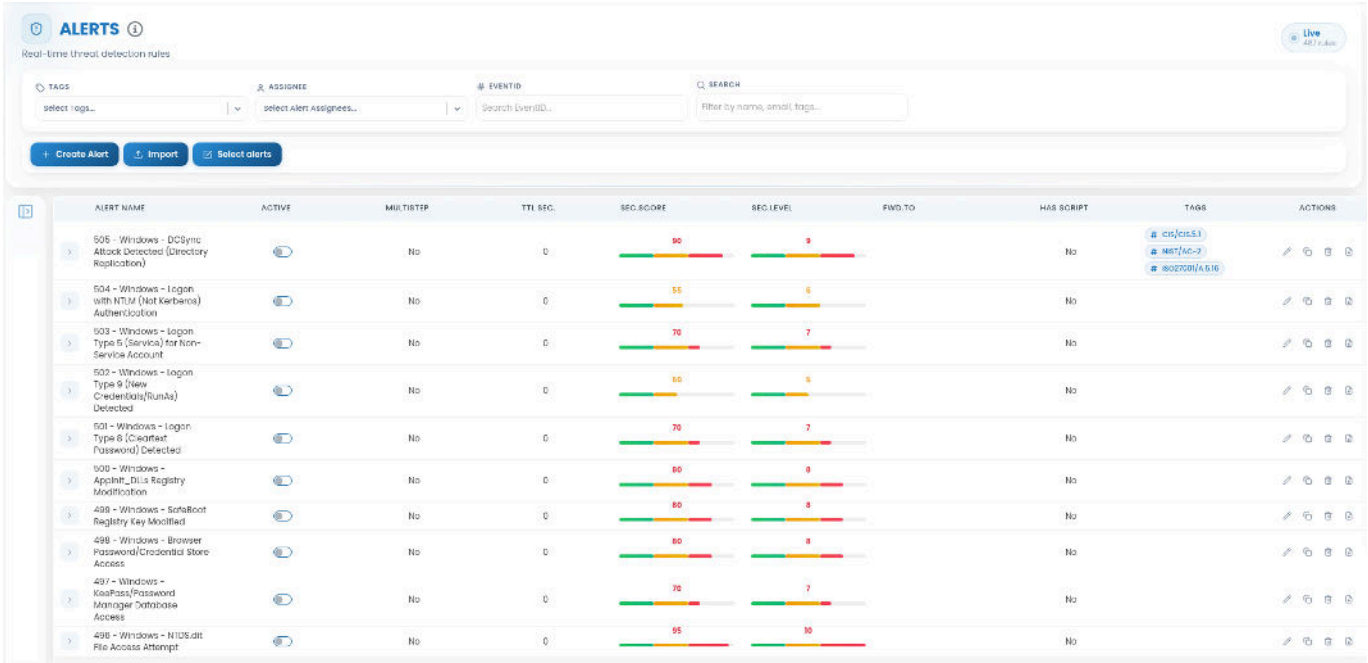


2. Configure Alerts Using the Inactive_accounts List

This section describes how to create a realtime alert that triggers whenever an inactive account appears in event data. The alert uses the previously created **Inactive_accounts** Object List as a correlation condition.

2.1 Access Realtime Alerts Configuration

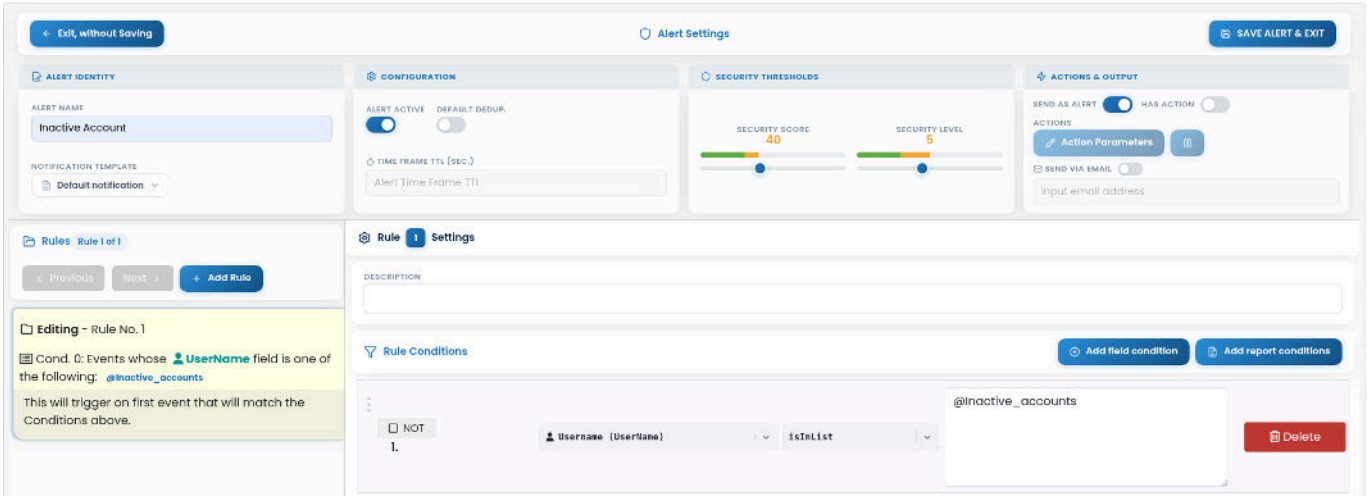
- Log in to CYBERQUEST with an account that has administrative or configuration permissions.
- Navigate to the menu: **Settings > Alerts > Realtime**, this opens the list of existing realtime alert rules.



3.2 Create a New Alert (or Duplicate an Existing One)

Click **CREATE ALERT** to create a new alert rule.

*Alternatively, select an existing authentication-related alert and click **Duplicate**, then rename it.*



This alert is designed to detect any activity generated by inactive or disabled user accounts. When an event contains a username that matches an entry inside the **Inactive_accounts** Object List, the alert will trigger immediately. This ensures the SOC is notified if any deprecated or unauthorized account is used across the environment.

***Note**: The "@" symbol placed before the list name (e.g., @Inactive_accounts) instructs the Data Correlation engine to reference a specific Object List, rather than treating the value as a literal list of strings. This ensures the alert evaluates the event username against all entries stored in the defined object list.*

Use the reports module to monitor specific actions by applying filters to an existing report.

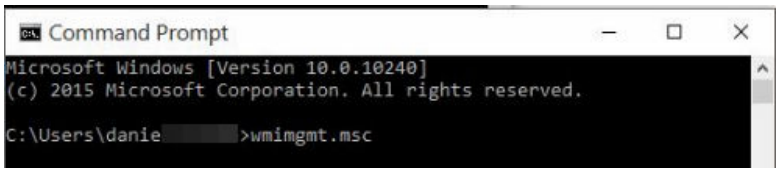
Operations · How to reconfigure WMI settings for remote collect

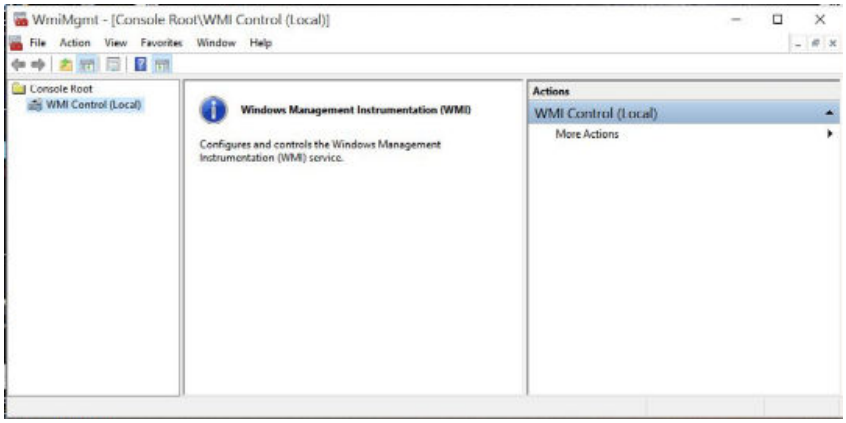
Adjust WMI namespace permissions on a Windows host to allow remote collection via CYBERQUEST agents.

1.Open the WMI Management Console on the target host

- Open a Command Prompt or Run dialog and execute:

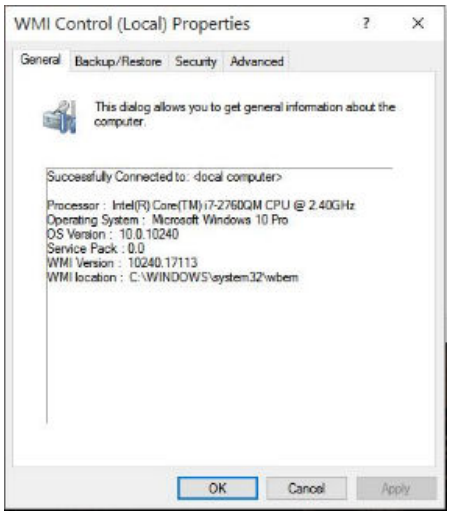
```
wmimgmt.msc
```





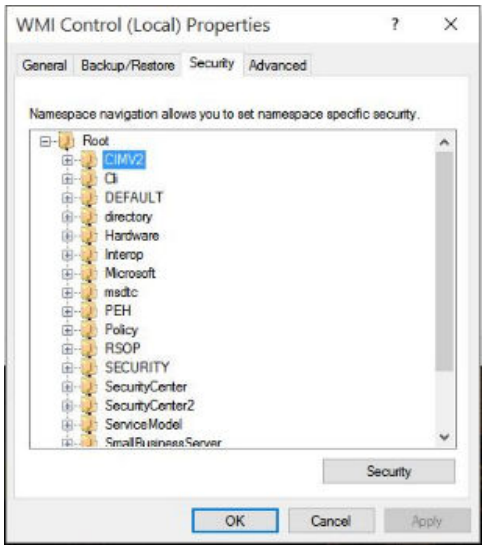
2.Open WMI Control properties

- In the console tree, right-click **WMI Control (Local)** and select **Properties**



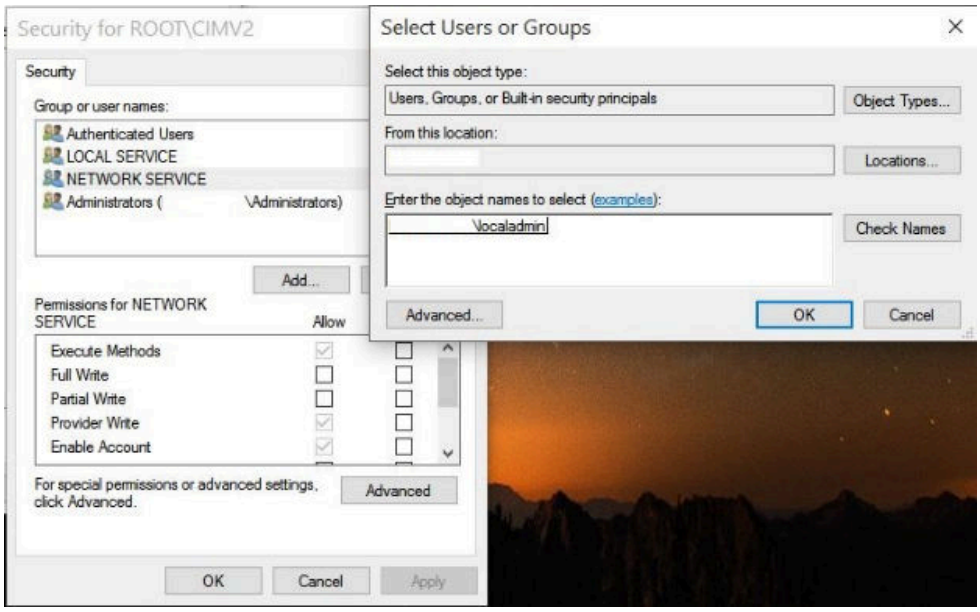
3.Select the CIMV2 namespace

- Go to the **Security** tab
- Select **ROOT \ CIMV2** and click **Security**



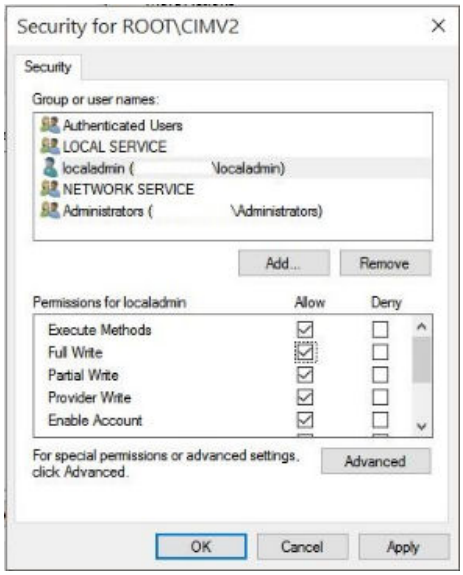
4.Add the collection account

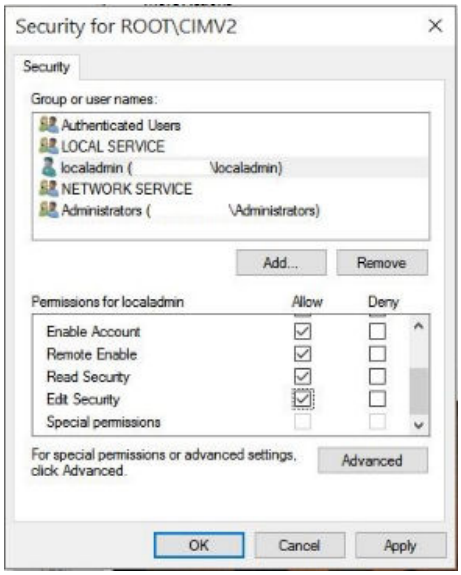
- Click **Add** and add the local user that will collect logs



5.Grant required permissions

- Select the added account and allow the required permissions (for example, **Enable Account**, **Remote Enable**, **Read Security**, **Execute Methods**)





For minimal permission sets, refer to:

[Minimum WMI permissions for Domain User Account]

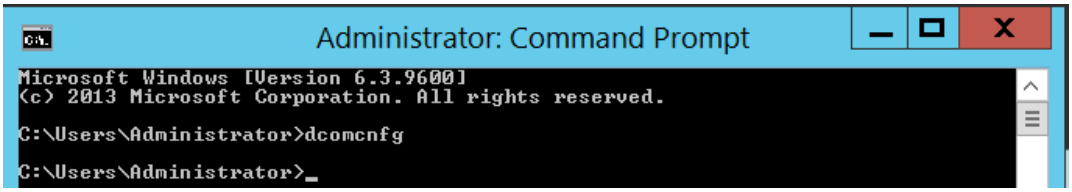
[Minimum WMI Permissions for Local User Account]

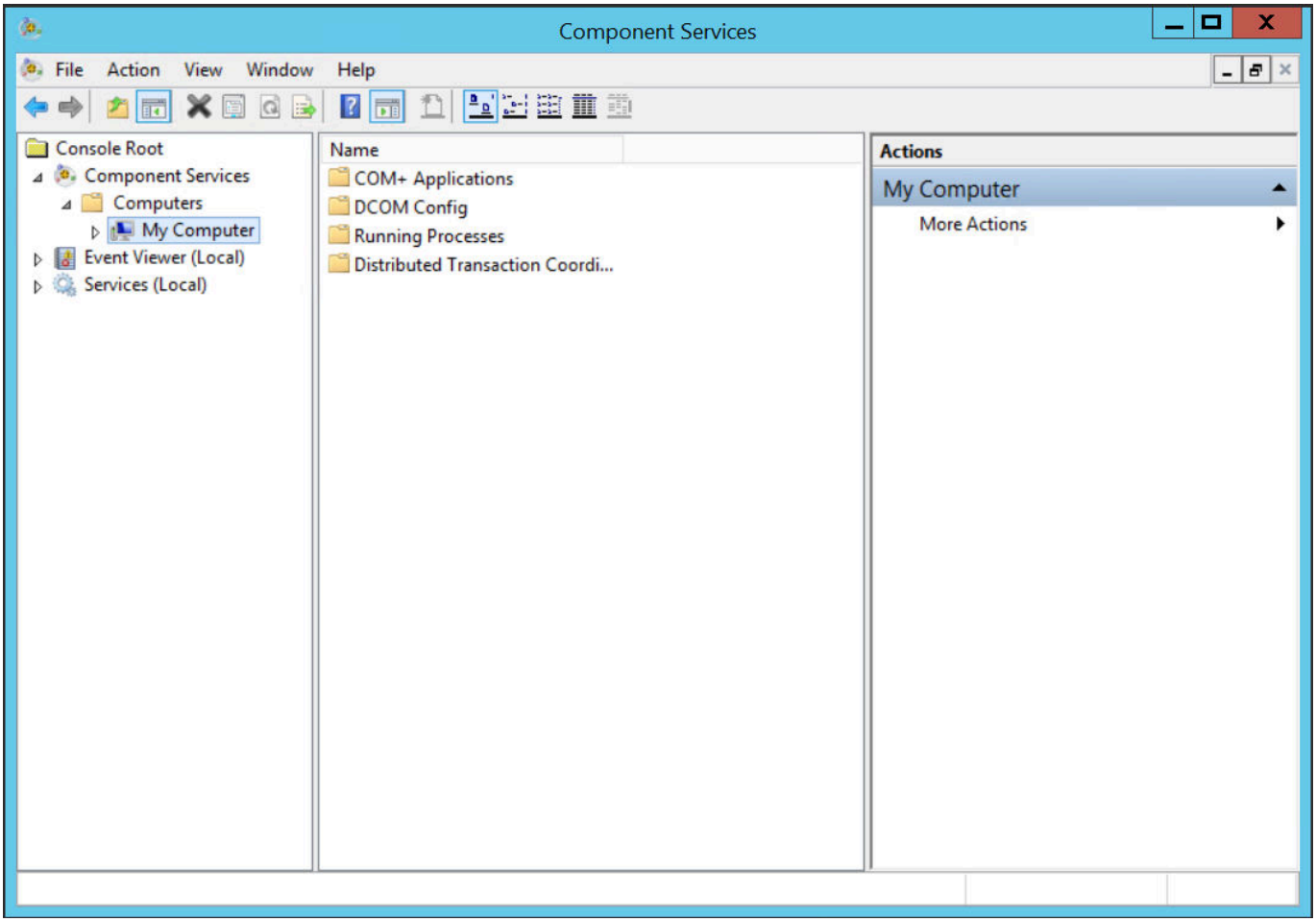
Operations · How to reconfigure WMI Settings Permissions for remote collect

1.Open Component Services

- Open the Run dialog or Command Prompt and execute:

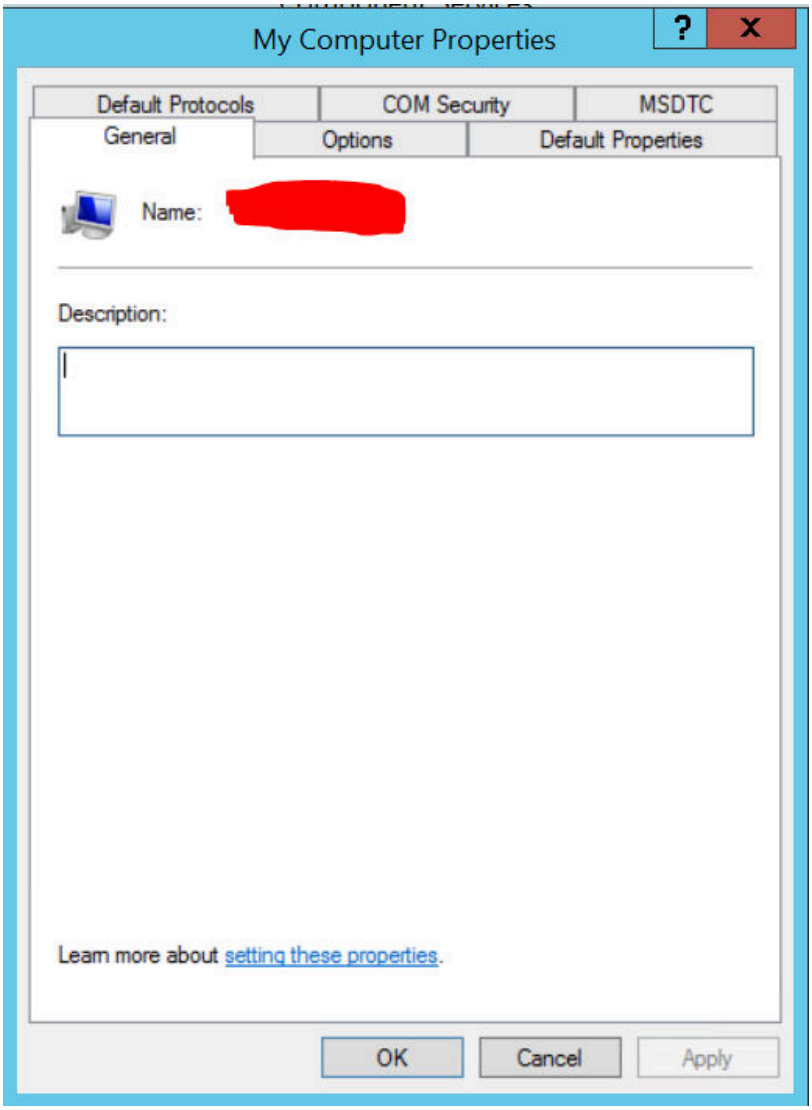
```
dcomcnfg
```





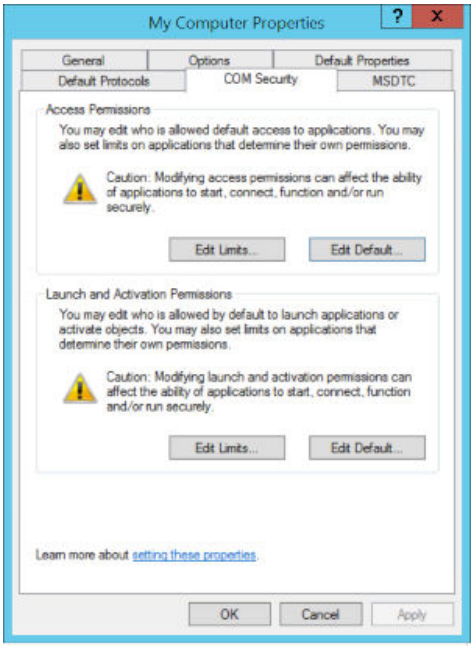
2.Navigate to **Component Services > Computers**

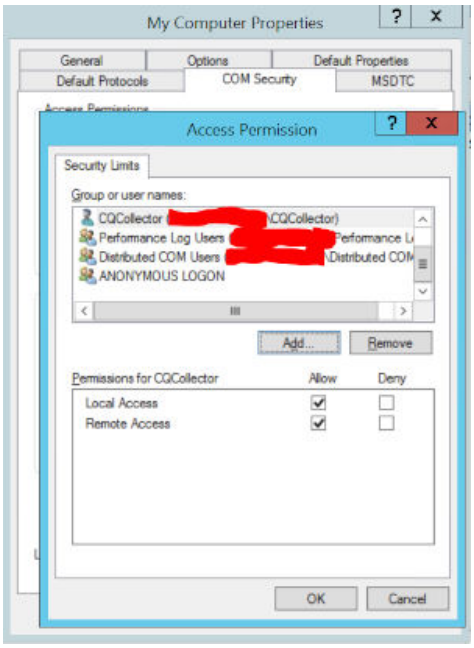
- Right-click **My Computer** and select **Properties**

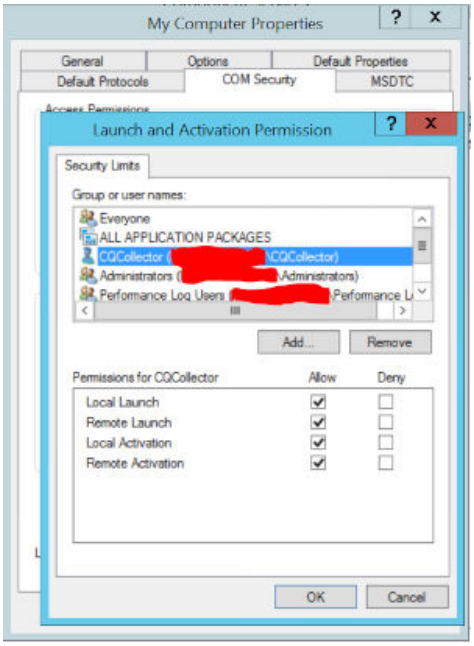


3.Go to the **COM Security** tab and click **Edit Limits** in both sections (Access Permissions and Launch and Activation Permissions)

- Add the collection account and allow **Remote Access**, **Remote Launch**, and **Remote Activation** as required

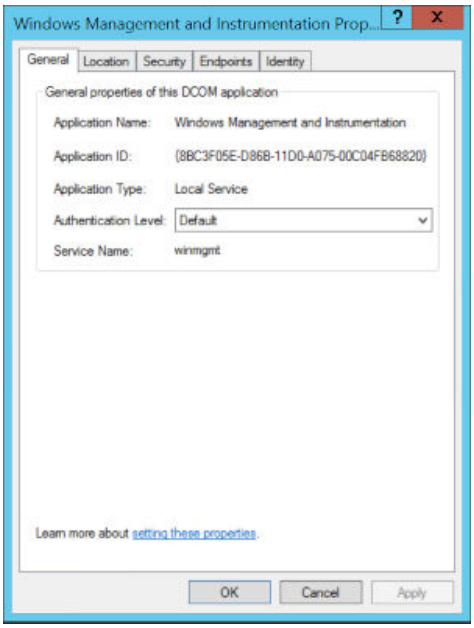




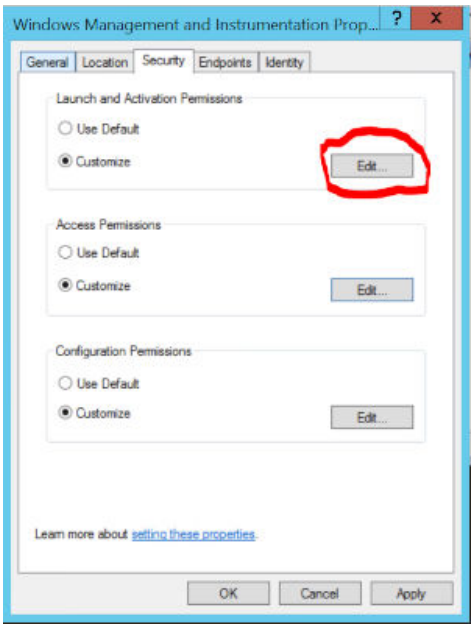


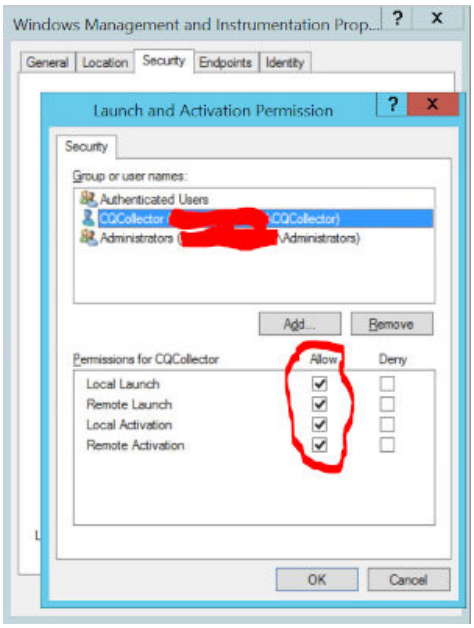
4.Configure WMI DCOM permissions

- In **Component Services**, expand **My Computer > DCOM Config**
- Locate **Windows Management Instrumentation**, right-click, and select **Properties**



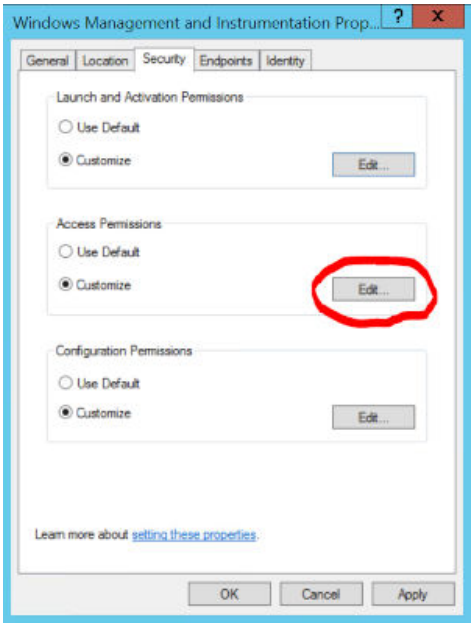
- Go to the **Security** tab and grant the collection account **Remote Launch** and **Remote Activation** where applicable

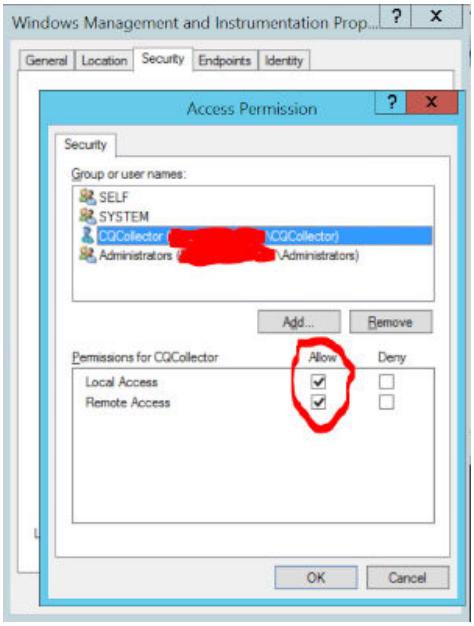




5.Edit access permissions

- In the same Security tab, edit Access Permissions to ensure the collection account has remote access rights





6.Verify required services and groups

- Confirm that **RemoteRegistry** and **Winmgmt** (Windows Management Instrumentation) services are running and set to **Startup type: Automatic**

7.Add the collection account to the following local groups:

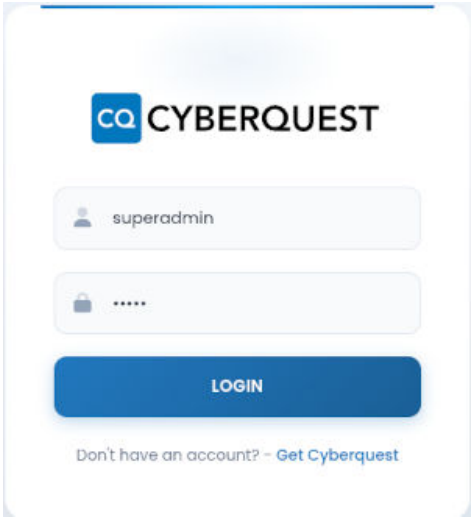
- **Event Log Readers**
- **Distributed COM Users**

Operations · How to restore data from archive

Restore archived events into an online or archive repository by creating an Import job.

Authentication

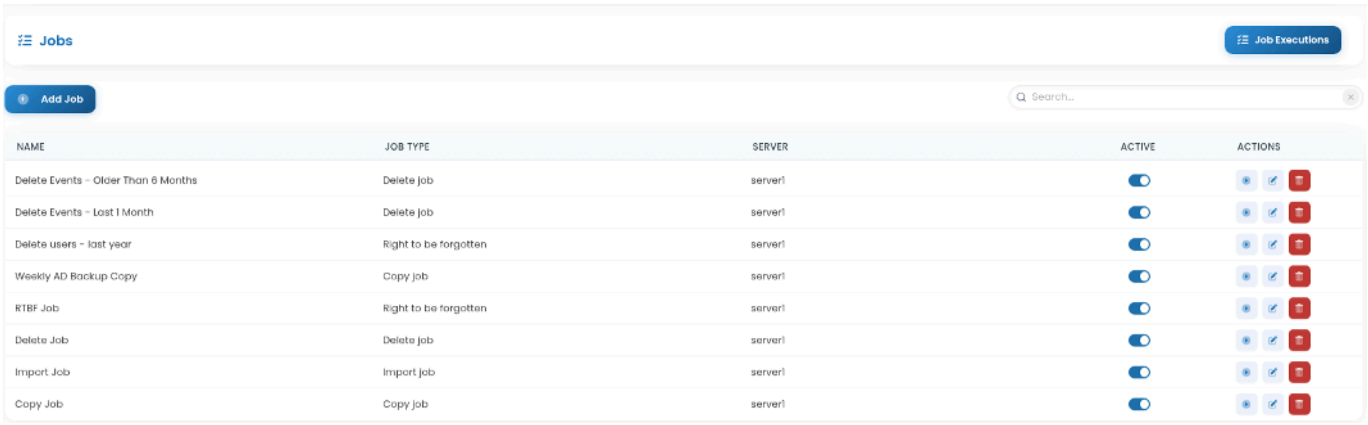
To access the web interface, open a browser and enter the application's IP address or DNS name (for example, ***https://CyberquestIPAddress***). The browser redirects to the CYBERQUEST authentication page:



Navigate to Settings

To create a new job, go to **Settings > Jobs** and select **Jobs**.

This page contains all job types added in the CYBERQUEST application.



Edit job: click Edit



button, similar to adding a job.

Start job: click Start



. Track status on the **Job Executions** page.

Delete job: click



and confirm.

To mark a job as activate/inactivate, press



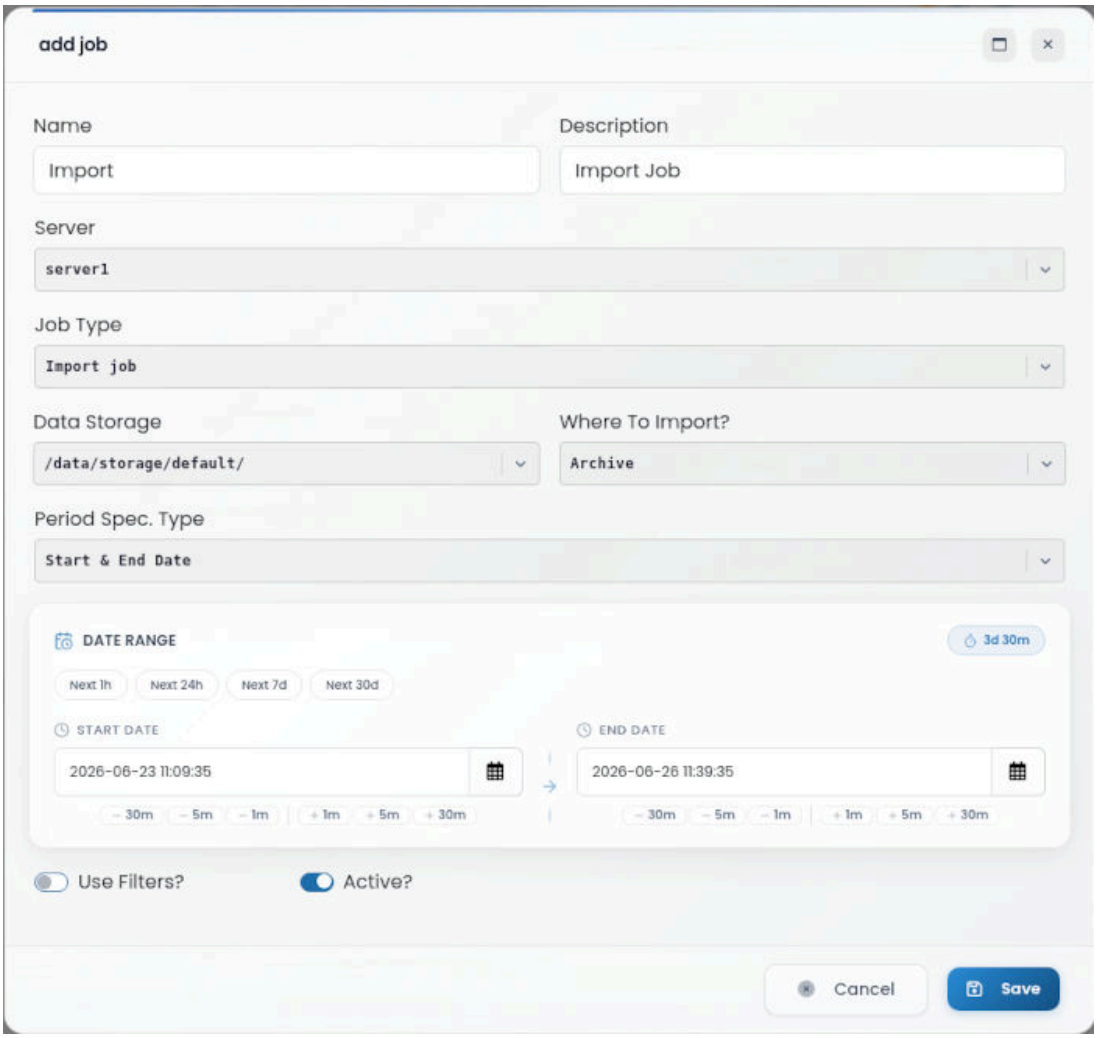
button.

Create an import job

Click the add button



to open the new job form.



Job fields:

- **Name:** Display name shown in the Jobs list
- **Description:** Short description of the restore/import operation
- **Server:** Data server where the job runs
- **Job Type:** Select **Import job**
  - **Import job:** Imports events from a source repository (archive) into an online or archive repository; useful for consolidation or decommissioning obsolete repositories
- **Data Storage:** Source data storage (archive) where events are read from
- **Where to Import:** Destination repository (online or offline) where events are written
- **Period Spec. Type:** Choose **Start & End Date** or **Last 'x' units**
  - **Start Date / End Date:** Exact time window to import

- **Last 'x' units:** Rolling window by seconds, minutes, hours, days, months, or years
- **Use Filters:** Add one or more AND/OR filter groups built under **Rules > Filter Rules** to restrict which events are imported
- **Active:** Mark the job active or inactive

When finished, click **Save** to apply changes or **Cancel** to discard.

Verify the job execution

Open **Job Executions** from the **Jobs** page using the Job Executions button:



Confirm the job status is completed and review the number of processed and imported events.

Operations · Website certificate import and Email certificate import

1. Exporting Windows certificate

Move or copy an SSL certificate from a Windows server to an Nginx server.

If you have multiple servers that need to use the same SSL certificate, such as in a load-balancer environment or using a wildcard or UC SSL certificates, you can export the certificate from the Windows certificate store to .pfx file and then convert the file to individual certificate and private key files and use it on an Nginx server. This may also be necessary when you switch hosting companies. We will be going over the exact process with step-by-step instructions in this article. If necessary, you can copy the SSL certificate from an Nginx server to a Windows server instead.

We will assume that you have already successfully installed the SSL certificate on the Windows web server. You will follow these steps to move or copy that working certificate to the Nginx server:

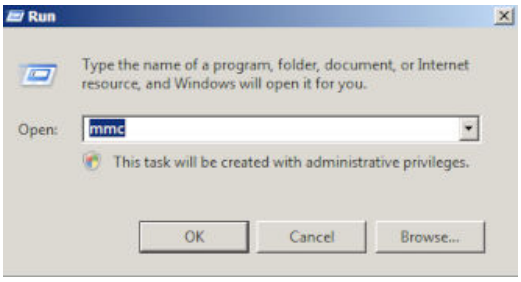
- **Export the SSL certificate** from the Windows server with the private key and any intermediate certificates into a .pfx file.
- **Convert the .pfx file** to individual certificates and private keys.
- **Import the SSL certificates** and private key on the new server.
- **Configure your Nginx web sites** to use the certificate.

The following screenshots are from a Windows Server 2008 machine but the instructions will also work for older (Windows Server 2003) and newer versions (Windows Server 2016).

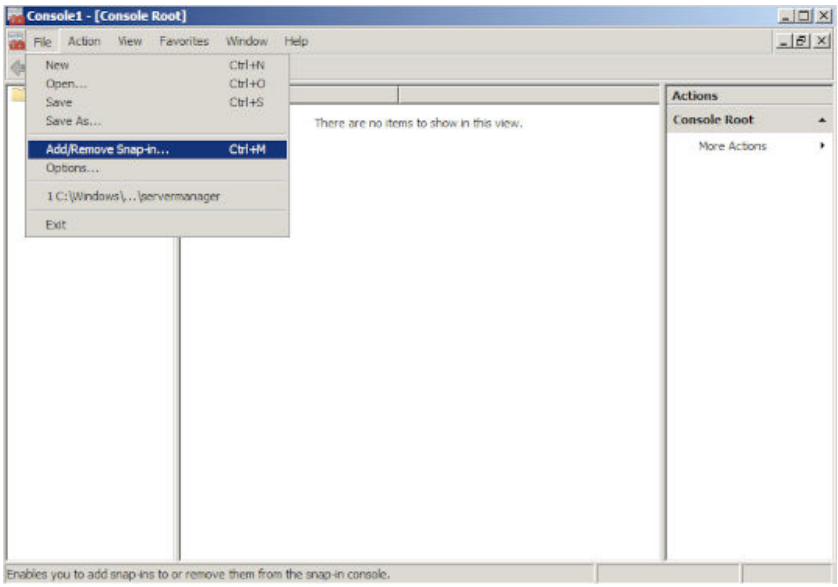
Export the certificate from the Windows MMC console

Note: These instructions will have you export the certificate using the MMC console. If you have Windows Server 2008 or higher (IIS7 or higher) you can also import and export certificates directly in the Server Certificates section in IIS.

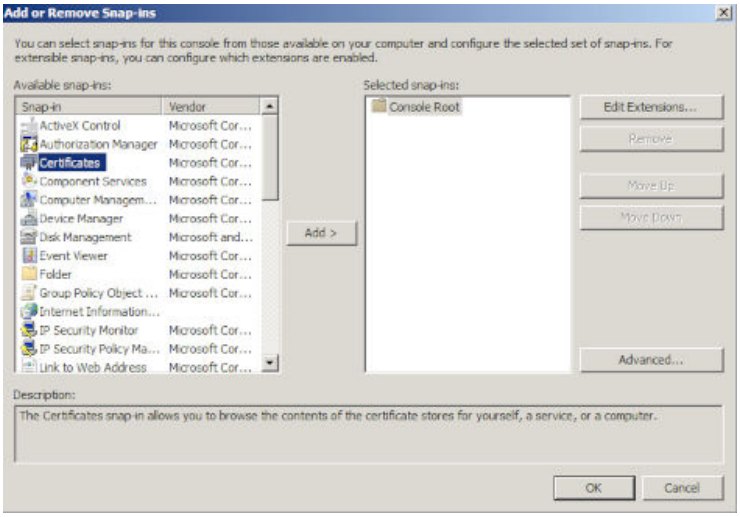
A.Click on the **Start menu** and open **Run** window. Type in **mmc** and click **OK.**



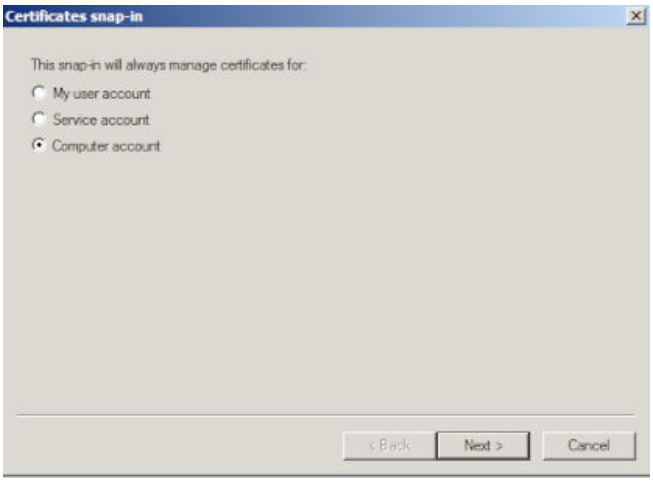
B.Click on the **File** menu and click **Add/Remove Snap-in…**



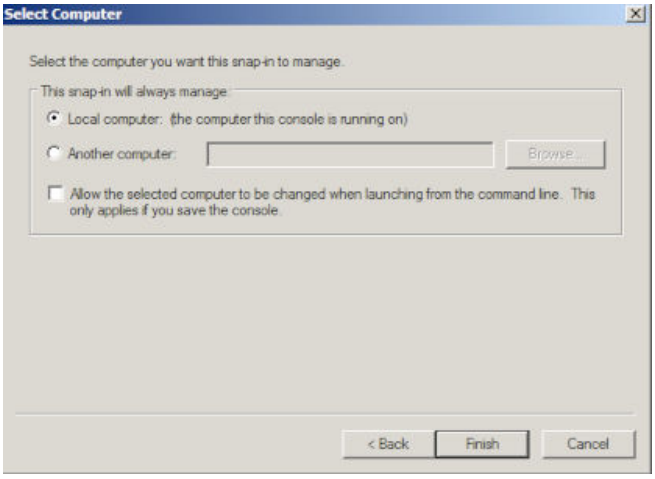
C.If you are using Windows Server 2003, click on the **Add** button. Double-click on **Certificates.**



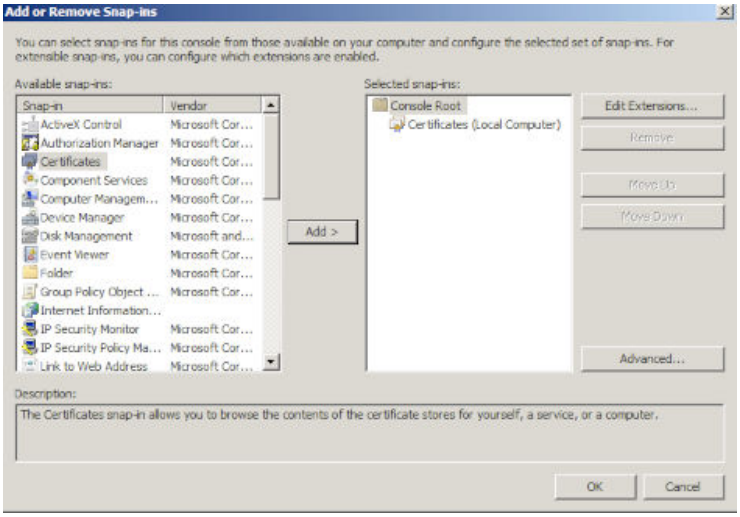
D.Click on **Computer Account** and click **Next.**



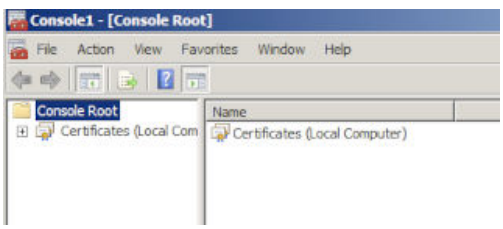
E.Leave **Local Computer** selected and click **Finish.**



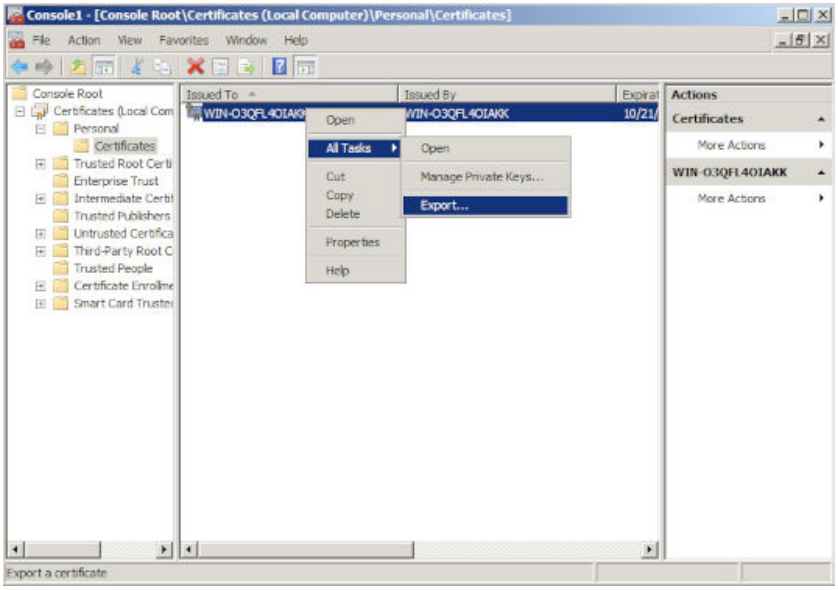
F.If you are using Windows Server 2003, click the **Close** button. Click **OK.**



G.Click the plus sign next to **Certificates** in the left pane.



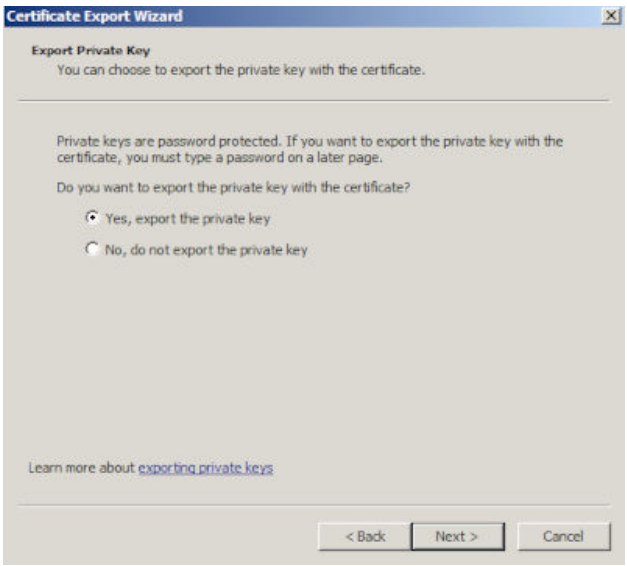
H.Click the plus sign next to the Personal folder and click on the **Certificates folder**. Right-click on the certificate you would like to export and select **All Tasks** and then **Export...**



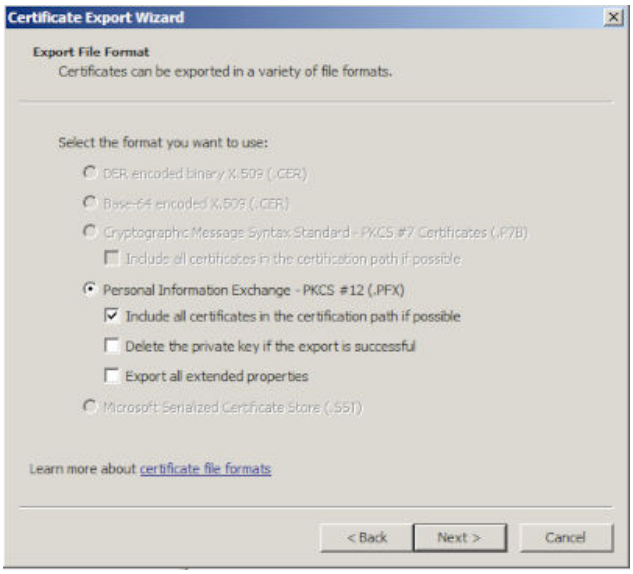
I.In the **Certificate Export Wizard** click **Next.**



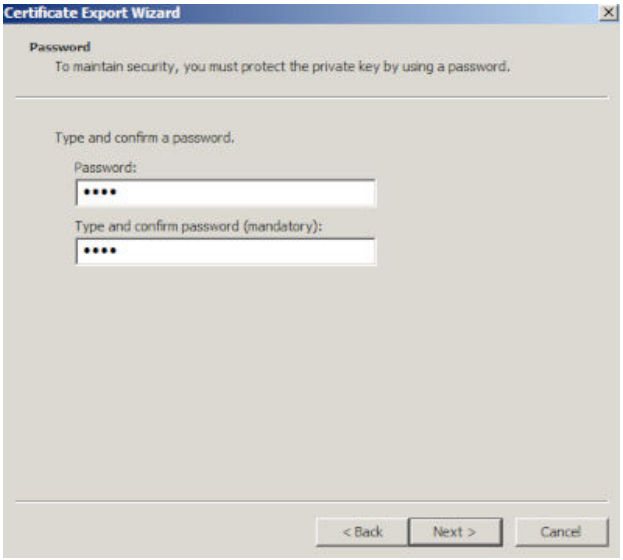
J.Choose **Yes, export the private key** and click **Next.**



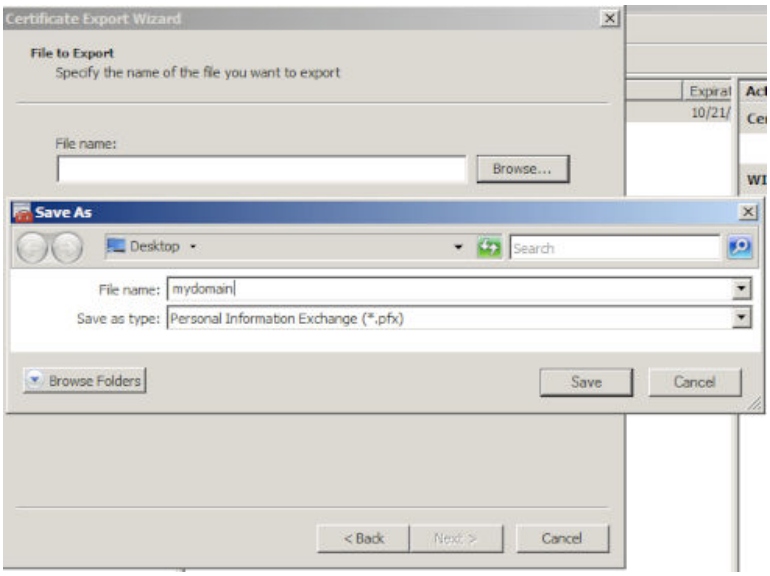
K.Click the checkbox next to **Include all certificates in the certification path if possible** and click **Next.**



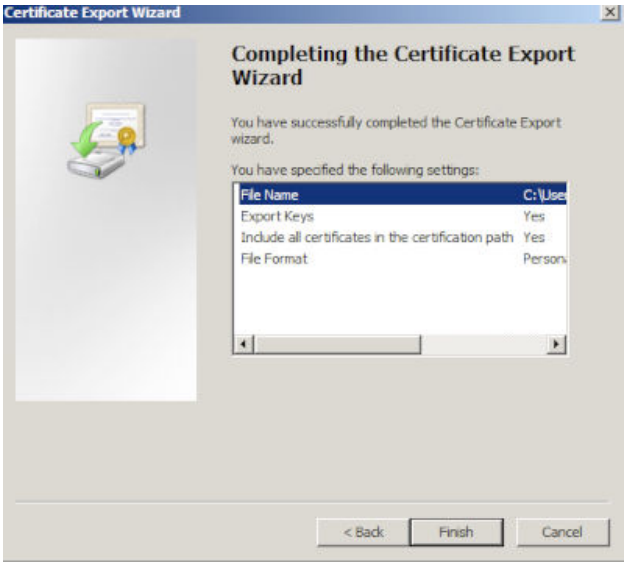
L.**Enter and confirm a password**. This password will be needed whenever the certificate is imported to another server.



M.Click **Browse** and find a location to save the .pfx file to. Type in a name such as **mydomain.pfx** and then click **Next.**



N.Click **Finish.** The .pfx file containing the certificates and the private key is now saved to the location you specified.



2. Convert Windows certificate to Linux certificate

Convert the .pfx file using OpenSSL

After you have exported the certificate from the Windows server you will need to extract all the individual certificates and private key from the .pfx file using OpenSSL (instead of using OpenSSL, you can use the SSL Converter to convert the .pfx file to a .pem file and then follow step 3).

1.Copy the .pfx file to the server or another computer that has OpenSSL installed.

2.Run this OpenSSL command to create a text file with the contents of the .pfx file:

```
openssl pkcs12 -in mydomain.pfx -out mydomain.txt -nodes
```

3.Open the **mydomain.txt** file that the command created in a text editor. Copy each certificate/private key to its own text file including the `bash"-----BEGIN RSA PRIVATE KEY-----"` and `bash"-----BEGIN CERTIFICATE-----"` headers. Save them with names such as **mydomain.key, mydomain.crt, intermediateCA.crt**, etc.

3.Assign SSL certificate to Linux webserver

Assigning the SSL certificate to a website

After you have converted the .pfx file, you will need to copy the newly created files to the Nginx server and edit your Nginx configuration file to use them. Just follow our Nginx SSL Installation instructions to do this.

Nginx SSL Installation instructions:

A.Edit the nginx configuration file using the following command:

```
nano /etc/nginx/sites-enabled/custom
```

A sample of the file is :

```
server {
    listen              443;
    ssl                 on;
    ** ssl_certificate      /etc/ssl/certs/myssl.crt; **
    ** ssl_certificate_key  /etc/ssl/private/myssl.key; **
    server_name me.com;
        root /var/opt/cyberquest/reports/app/webroot;
        index index.php index.html index.htm;
 location / {
        try_files $uri $uri/ /index.php?$args;
    }
```

B.In order to include the recently exported certificate replace the path of the default certificate and key:

```
    ** ssl_certificate      /etc/ssl/certs/ mydomain.crt; **
    ** ssl_certificate_key  /etc/ssl/private/ mydomain.key; **
```

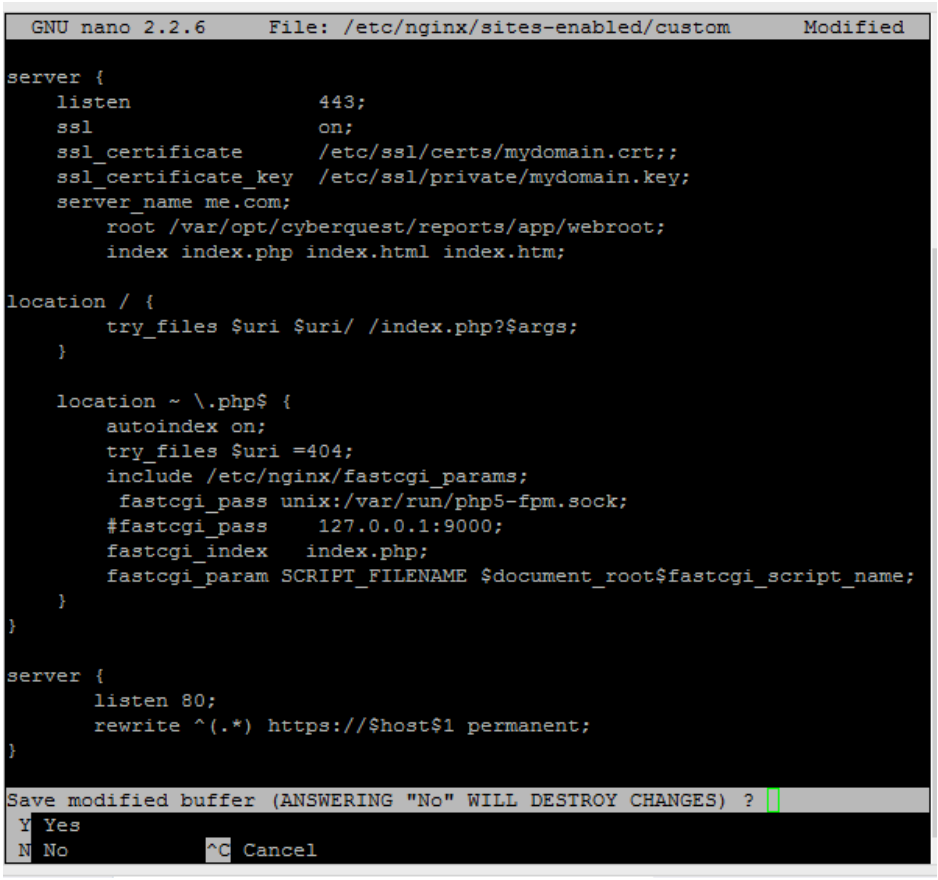
```
server {
    listen              443;
    ssl                 on;
    ssl_certificate      /etc/ssl/certs/myssl.crt;
    ssl_certificate_key  /etc/ssl/private/myssl.key;
    server_name me.com;
        root /var/opt/cyberquest/reports/app/webroot;
        index index.php index.html index.htm;

location / {
        try_files $uri $uri/ /index.php?$args;
    }

    location ~ \.php$ {
        autoindex on;
        try_files $uri =404;
        include /etc/nginx/fastcgi_params;
         fastcgi_pass unix:/var/run/php5-fpm.sock;
        #fastcgi_pass    127.0.0.1:9000;
        fastcgi_index   index.php;
        fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
    }
}

server {
       listen 80;
       rewrite ^(.*) https://$host$1 permanent;
}
```

C.Save the configuration file.



D.Restart Nginx service using the following command:

```
systemctl restart nginx.service
```

While there are several steps in the process, moving an SSL certificate from one Windows server to an Nginx server is quite simple. It involves exporting a working SSL certificate from the MMC console to a .pfx file which contains the certificates and private key and then converting that file to separate files. You can then copy the files to the Nginx server and install the certificate like normal. If you need to move your SSL certificate to or from a different type of server, select the server type on our main SSL Certificate Import/Export Page.

4. Assign SSL certificate to Linux mail server

4.1. Import a certificate from a pfx file e.g. exported from a Windows server

```
root@me:~# openssl pkcs12 -in ExportWithPrivate.pfx -clcerts -nokeys -out mydomain.crt
```

IMPORTANT - These files are to be kept SECRET.

```
root@me:~# openssl pkcs12 -in ExportWithPrivate.pfx -out servername.pem
```

```
root@me:~# openssl rsa -in servername.pem -out exim.key
```

Now concatenate the certificates:

```
root@me:~# cat mydomain.crt /etc/ssl/certs/ca-certificates.crt > exim.crt
```

Copy the files **exim.key** and **exim.crt** to the following path: **/etc/exim**

IMPORTANT: Backup the files to a secure location and delete the remaining files.

4.2. Update Exim configuration files

For split-file configuration **(debian only)**, edit the file: **/etc/exim4/conf.d/main/03_exim4-config_tlsoptions** and uncomment the following lines:

```
#log_selector = +tls_cipher +tls_peerdn
#tls_advertise_hosts = *
#tls_certificate = CONFDIR/exim.crt
#tls_privatekey = CONFDIR/exim.key
```

Then, activate the exim4 changes by:

```
update-exim4.conf
```

Change the file security so that only exim can read them (if you are running as exim):

```
root@myserver:~# chmod 600 exim.*
```

```
root@myserver:~# chown exim exim.*
```

In either case you need to restart exim:

```
systemctl restart exim4.service
```

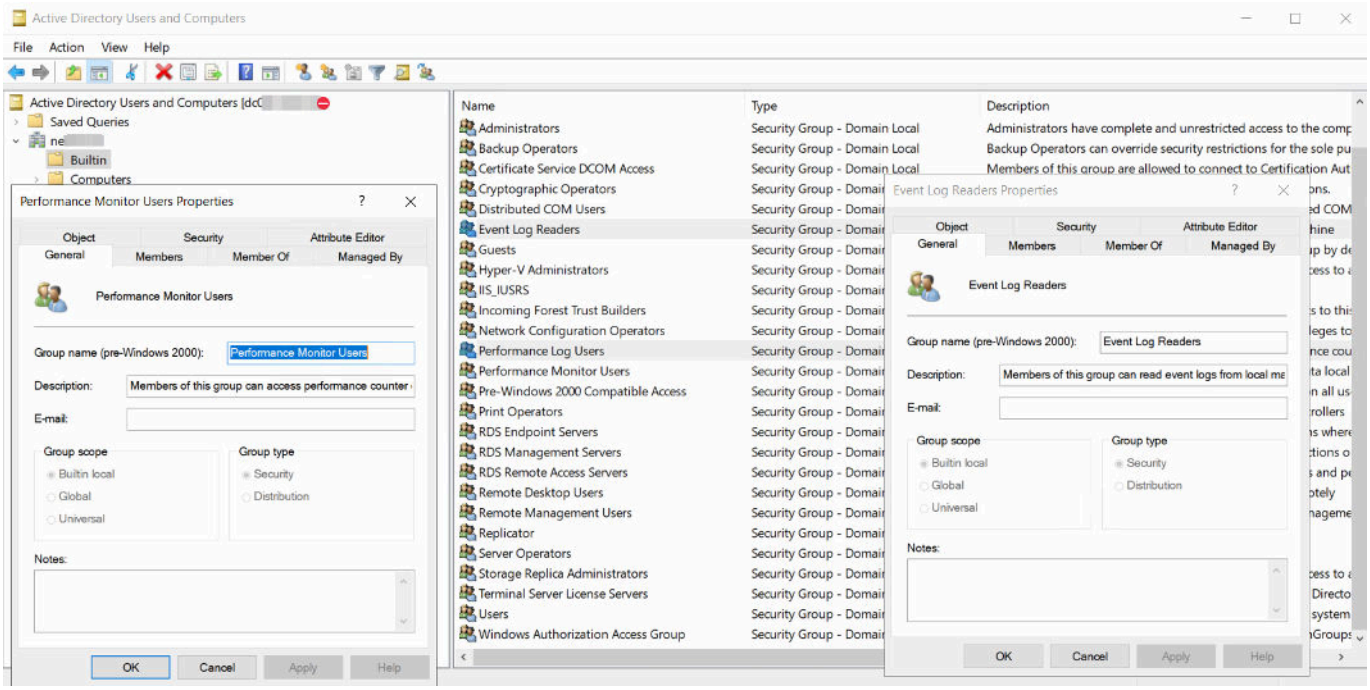
https://github.com/Exim/exim/wiki/_preview (https://github.com/Exim/exim/wiki/_preview)

Operations · Minimum WMI permissions for Domain User Account

In order to collect events from a windows machine, consider a user account that is already a member of the “Domain Users” group.

Next you will have to allow remote WMI access to use it as a service account with restricted permissions.

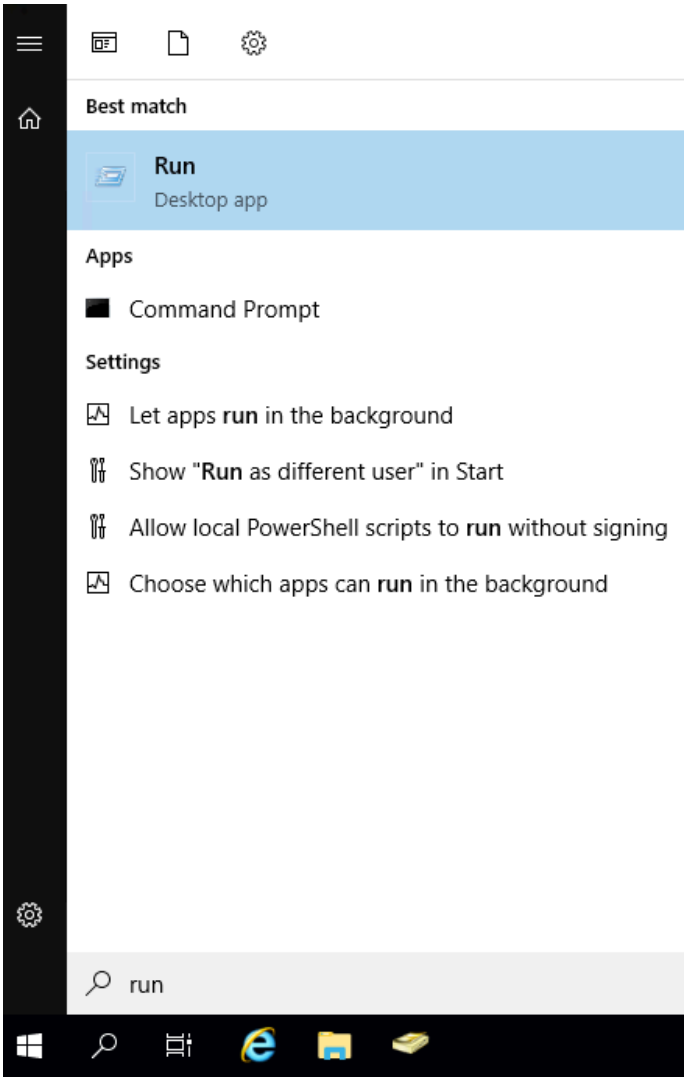
First, add the user account to the Domain Groups named “Performance Log Users” and “Event Log Readers”.

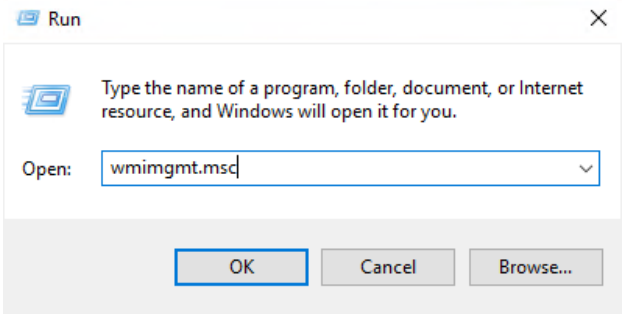


Next, set up the access permissions for the user account in the WMI Control configuration:

1.Open the WMI Control console:

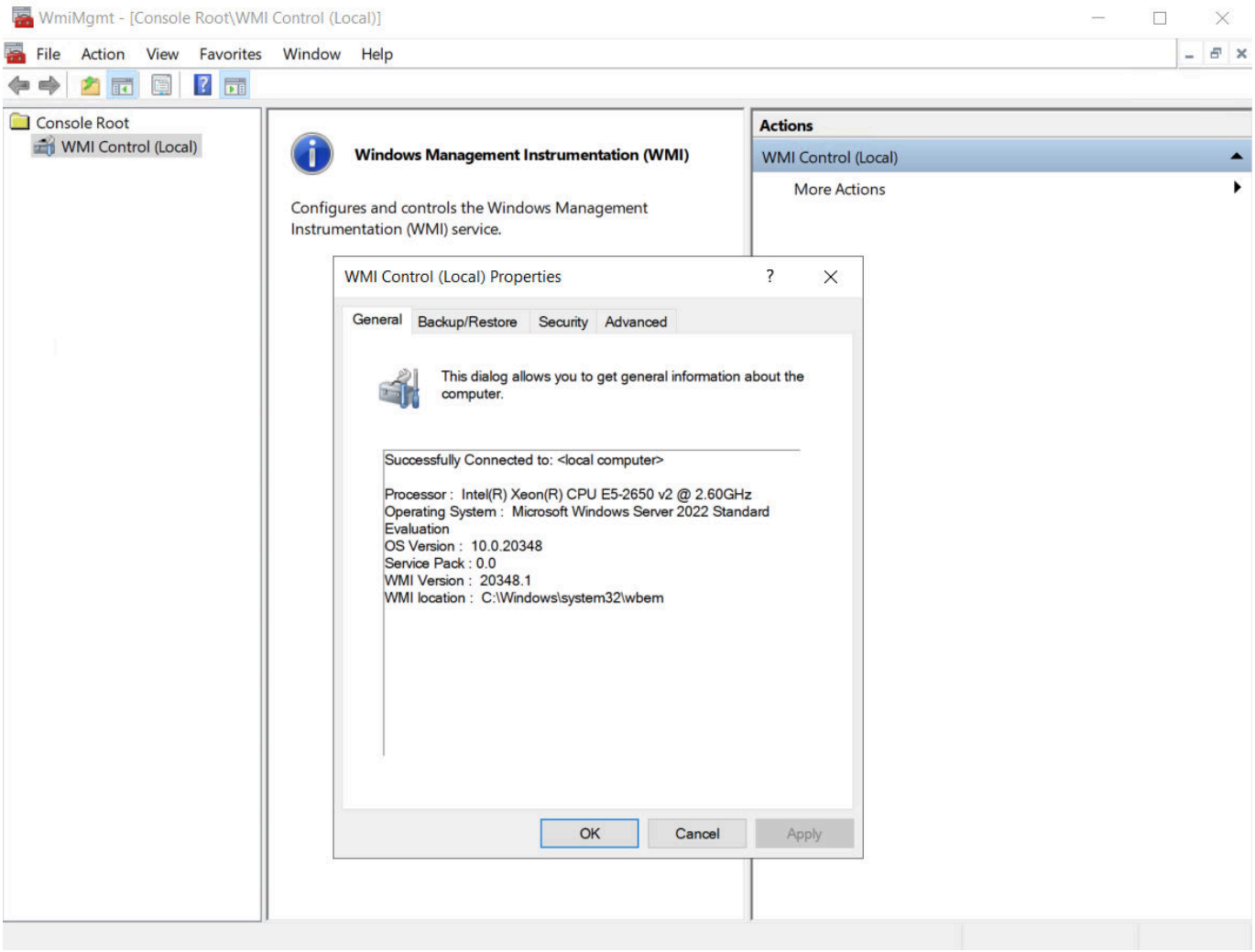
Click Start, search for “Run” and type wmimgmt.msc, then click OK.



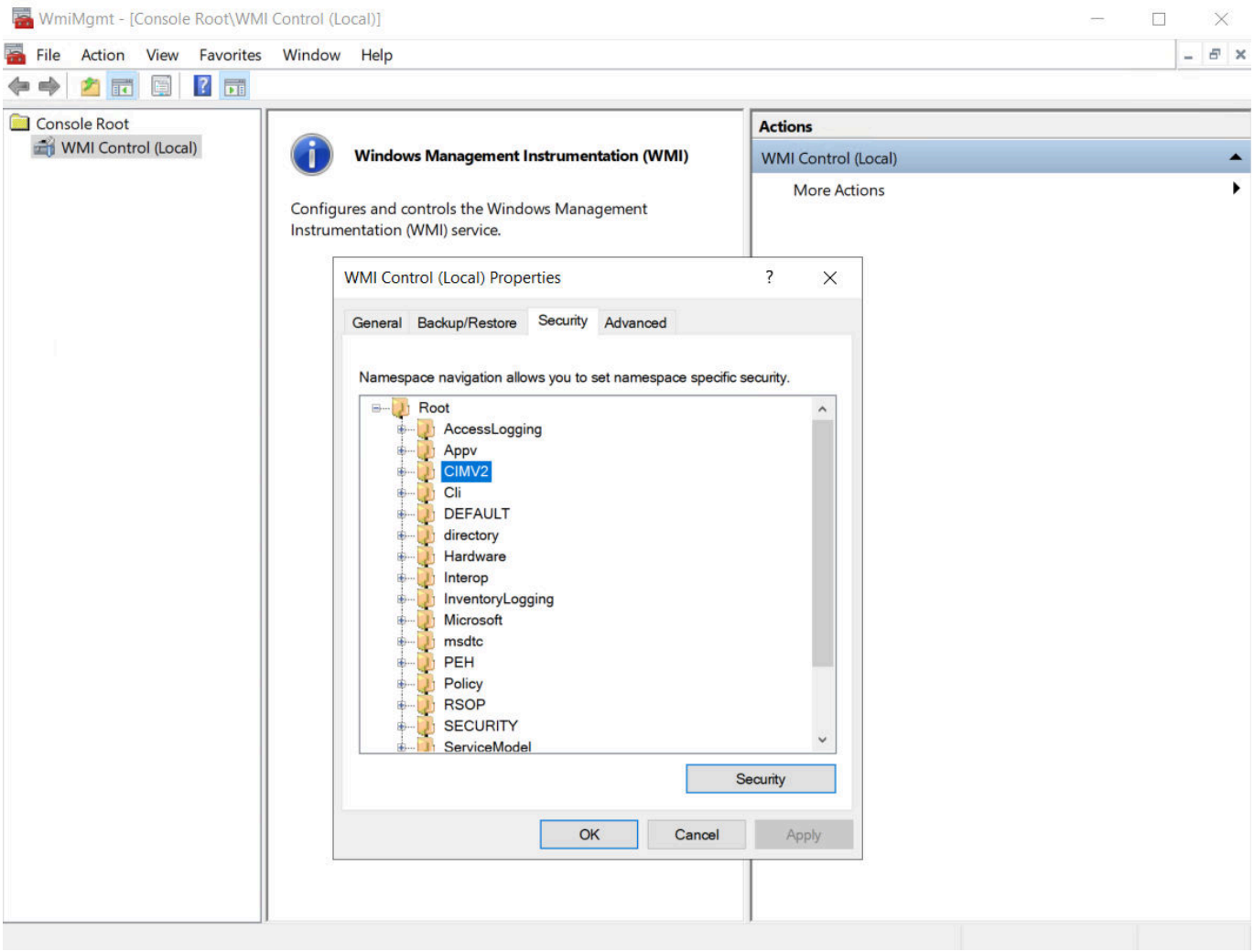


2.In the console tree, right-click WMI Control and then click Properties.

3.Click the Security tab.

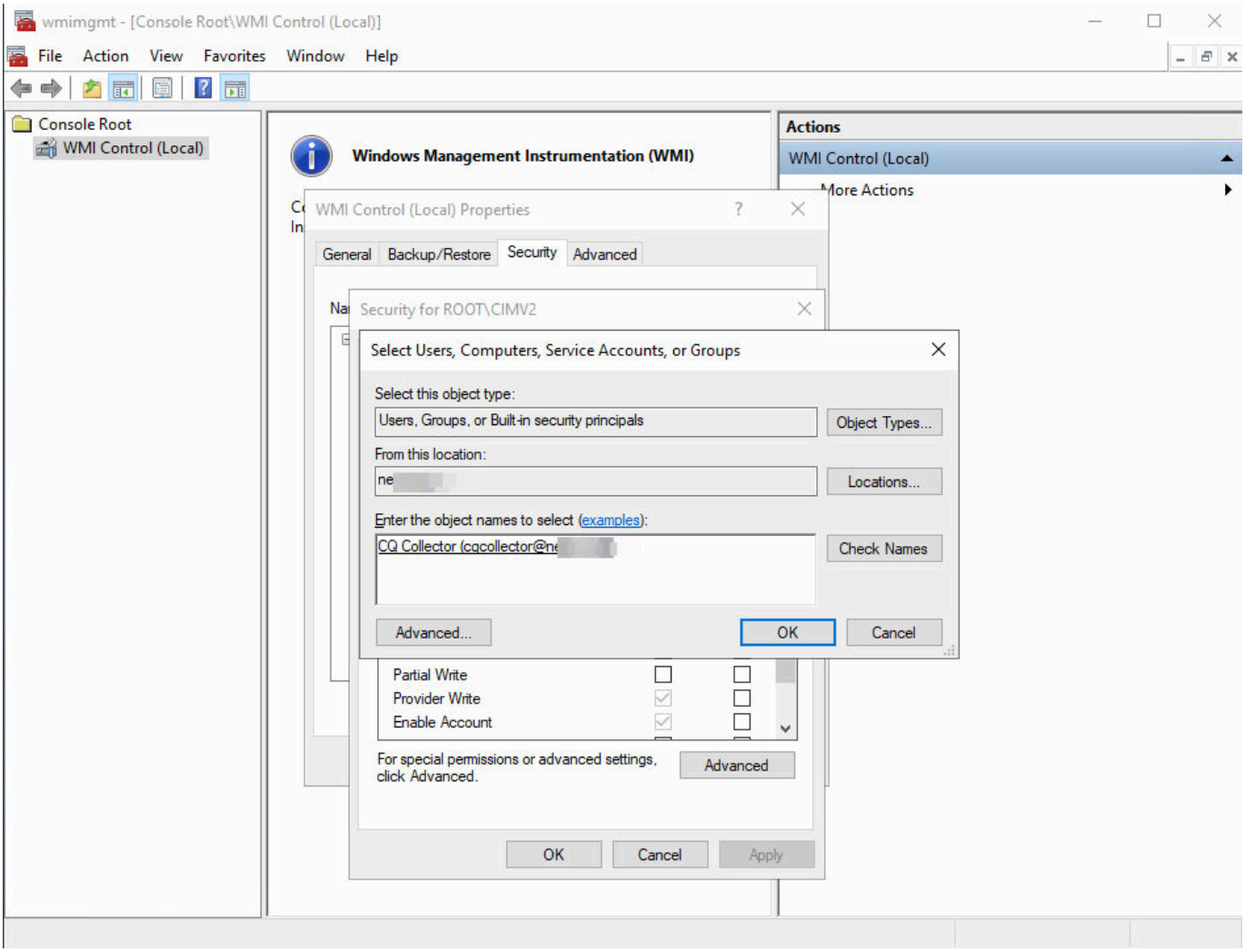


4.Navigate and select the "\Root\CIMV2" namespace to choose which user or group will have access, and then click on Security button.



In the Security dialog box, click Add.

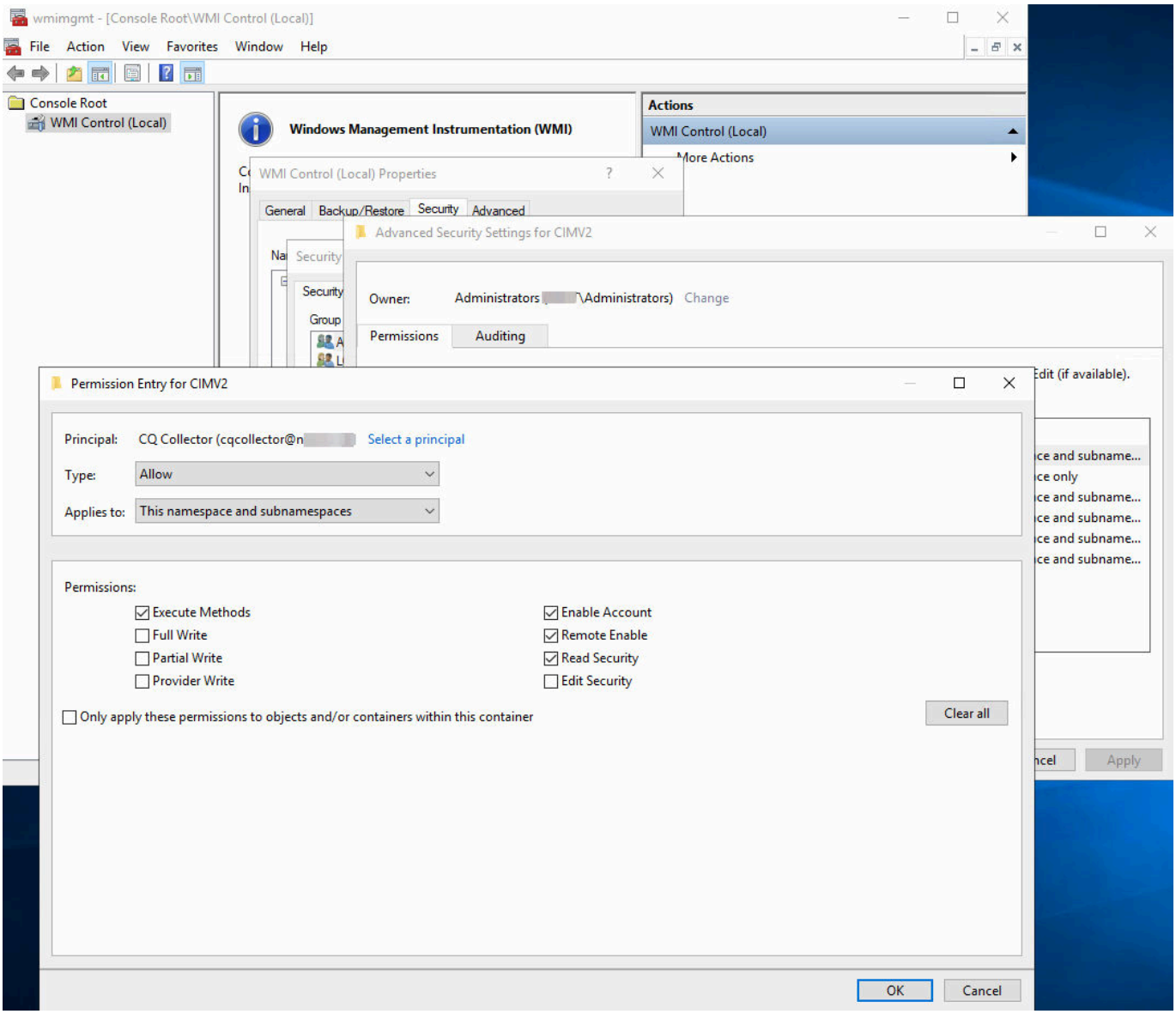
In the Select Users, Computers, or Groups dialog box, enter the name of the object (user or group) that you want to add, click OK and then choose Advanced.



In the Advanced Security dialog box under Permissions, edit the permissions and check the following check boxes:

- “Execute Methods”
- “Enable Account”
- “Remote Enable”
- “Read Security”

Select Apply to “This namespace and subnamespaces”:

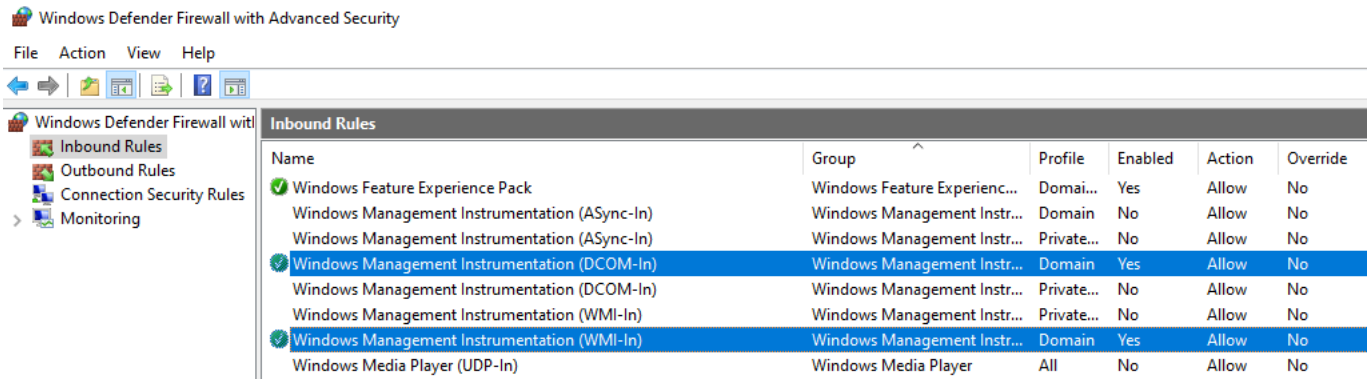


Click OK 4 times to close all the windows.

Windows Firewall Rules for Inbound and Outbound

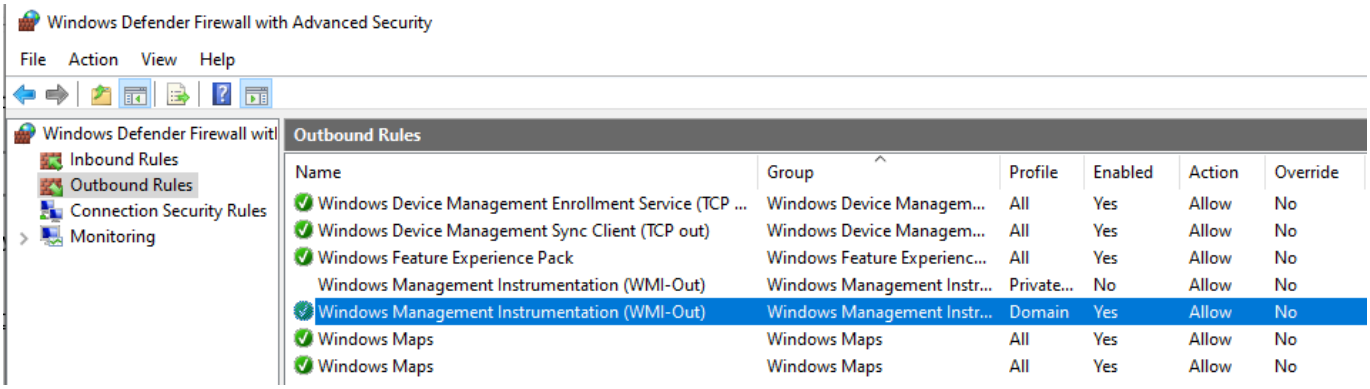
Enable the following rules on Inbound:

- Windows Management Instrumentation (DCOM-In)
- Windows Management Instrumentation (WMI-In)



Enable the following rules on Outbound:

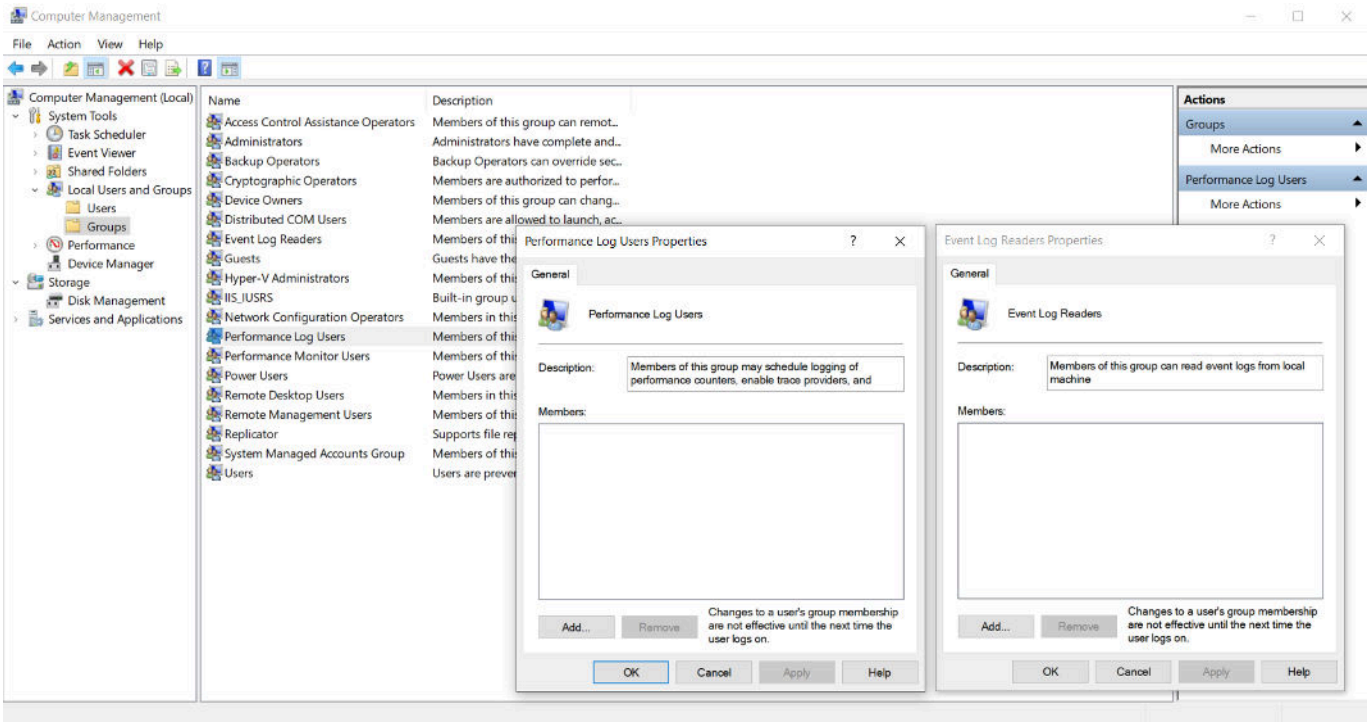
- Windows Management Instrumentation (WMI-Out)



Operations · Minimum WMI Permissions for Local User Account

To allow the user account to be used as a service account with limited permissions, remote WMI access must be enabled.

First, add the user account to the local group named “Performance Log Users” and “Event Log Readers”.

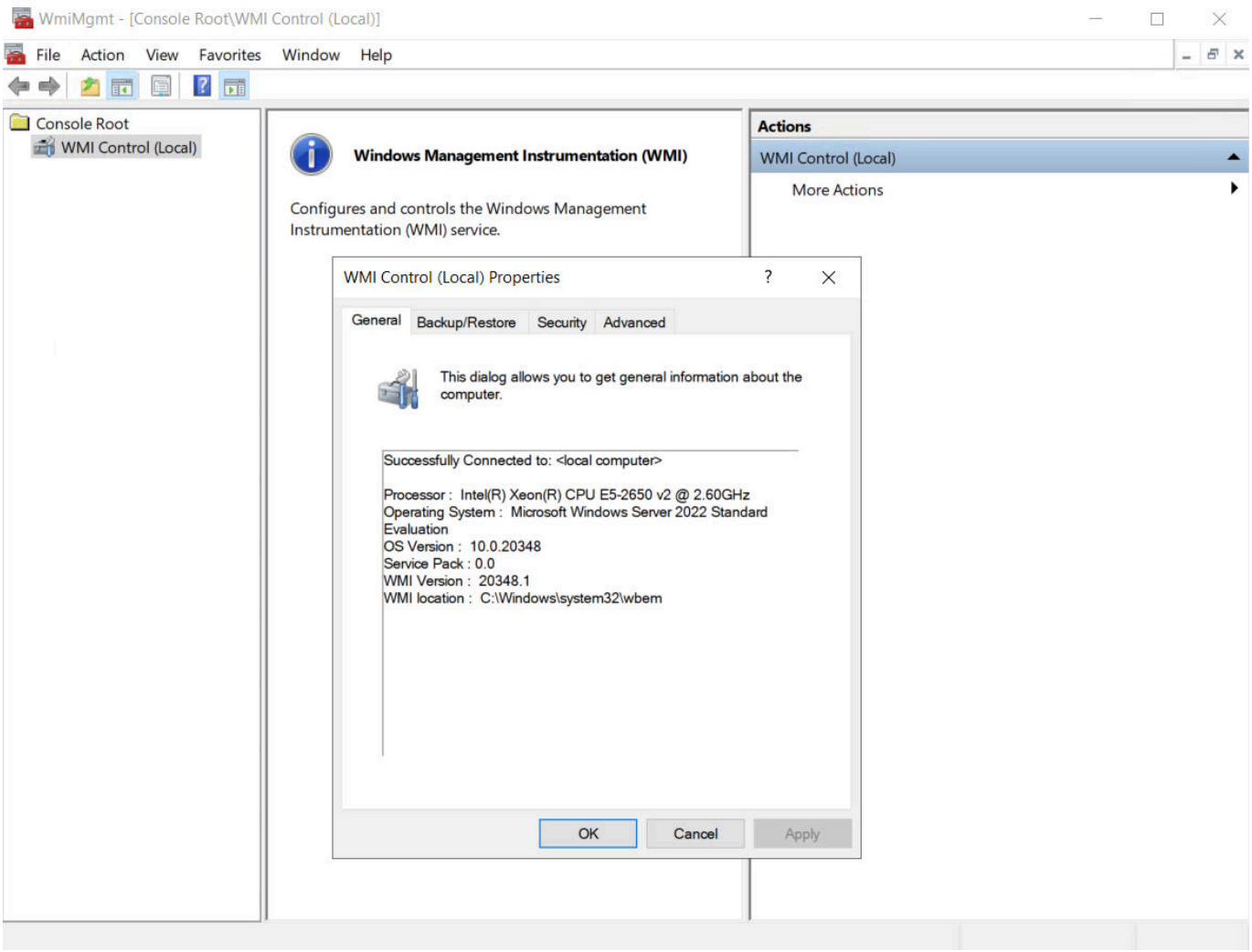


Next, set up the access permissions for the user account in the WMI Control configuration:

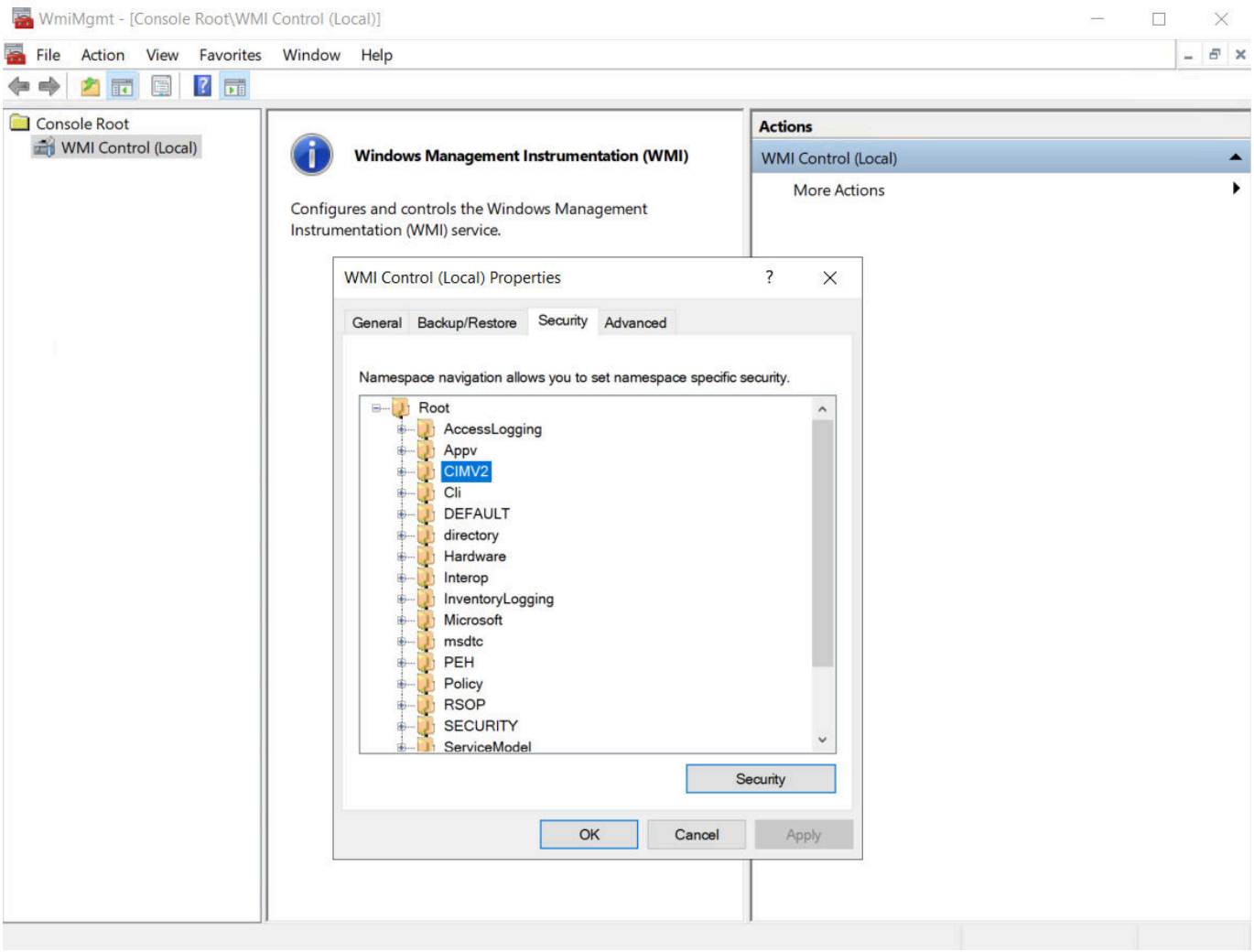
1.Open the WMI Control console: Click Start, choose Run and type wmimgmt.msc, then click OK.

2.In the console tree, right-click WMI Control and then click Properties.

3.Click the Security tab.

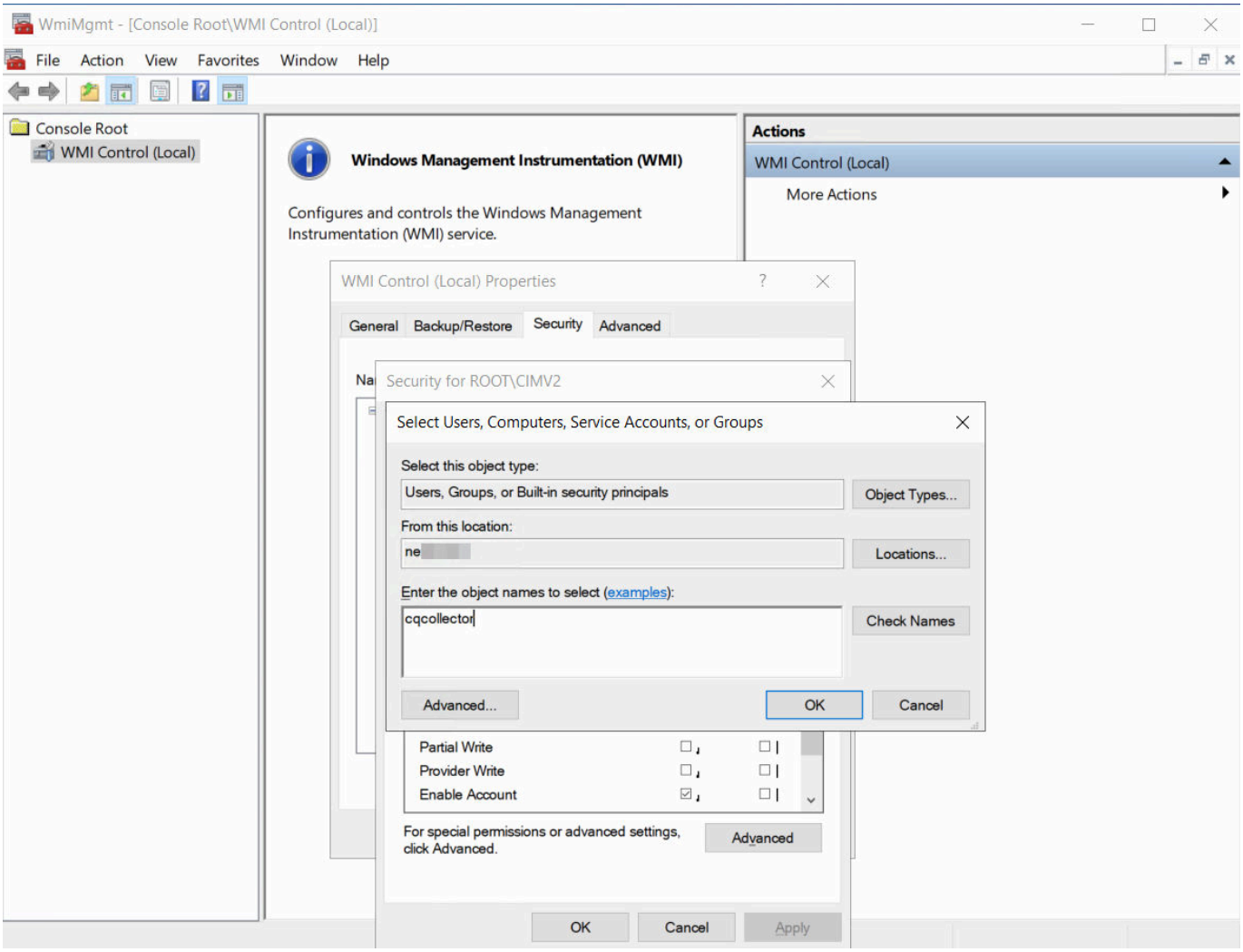


Select the "\Root\CIMV2" namespace to choose which user or group will have access, and then click on Security.

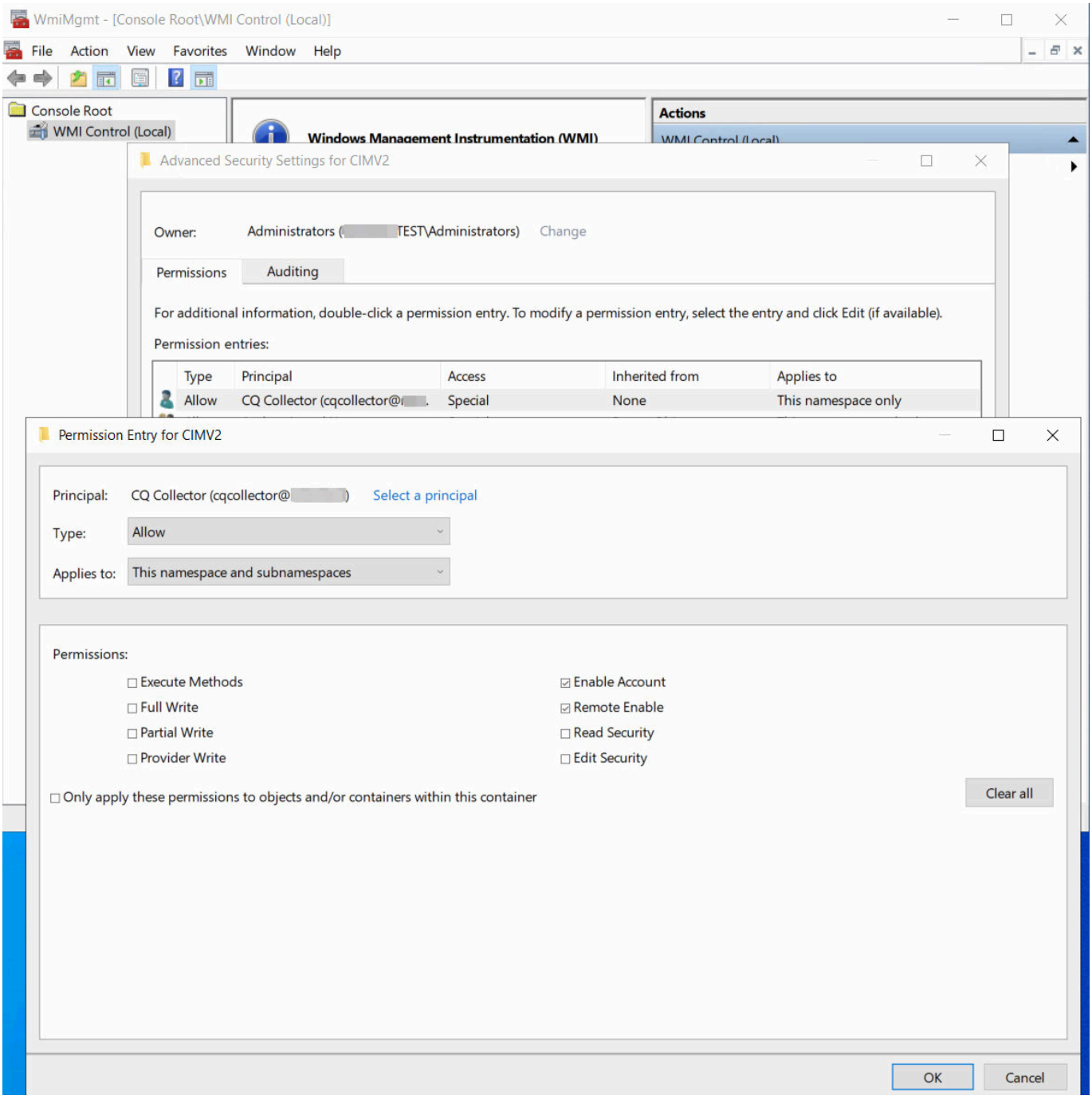


In the Security dialog box, click Add.

In the Select Users, Computers, or Groups dialog box, enter the name of the object (user or group) that you want to add, click OK and then choose Advanced.



In the Advanced Security dialog box under Permissions, edit the permissions and check the “Enable Account” and “Remote Enable” boxes. Select Apply to “This namespace and subnamespaces”:



Click OK 4 times to close all the windows.

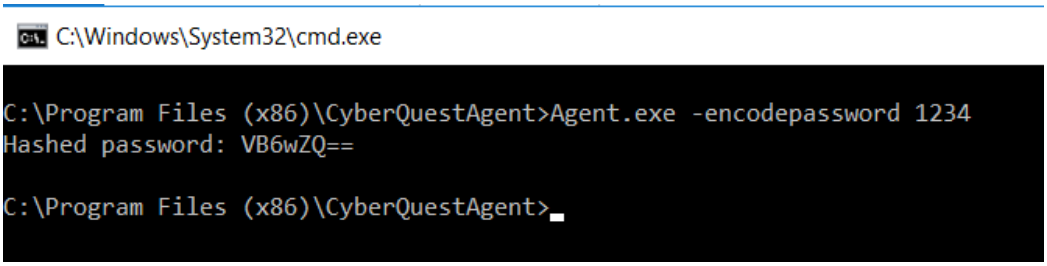
And now you're finished! The user now has remote access to WMI information.

Operations · Password encoding

How to encode a password for collecting events from domain computers

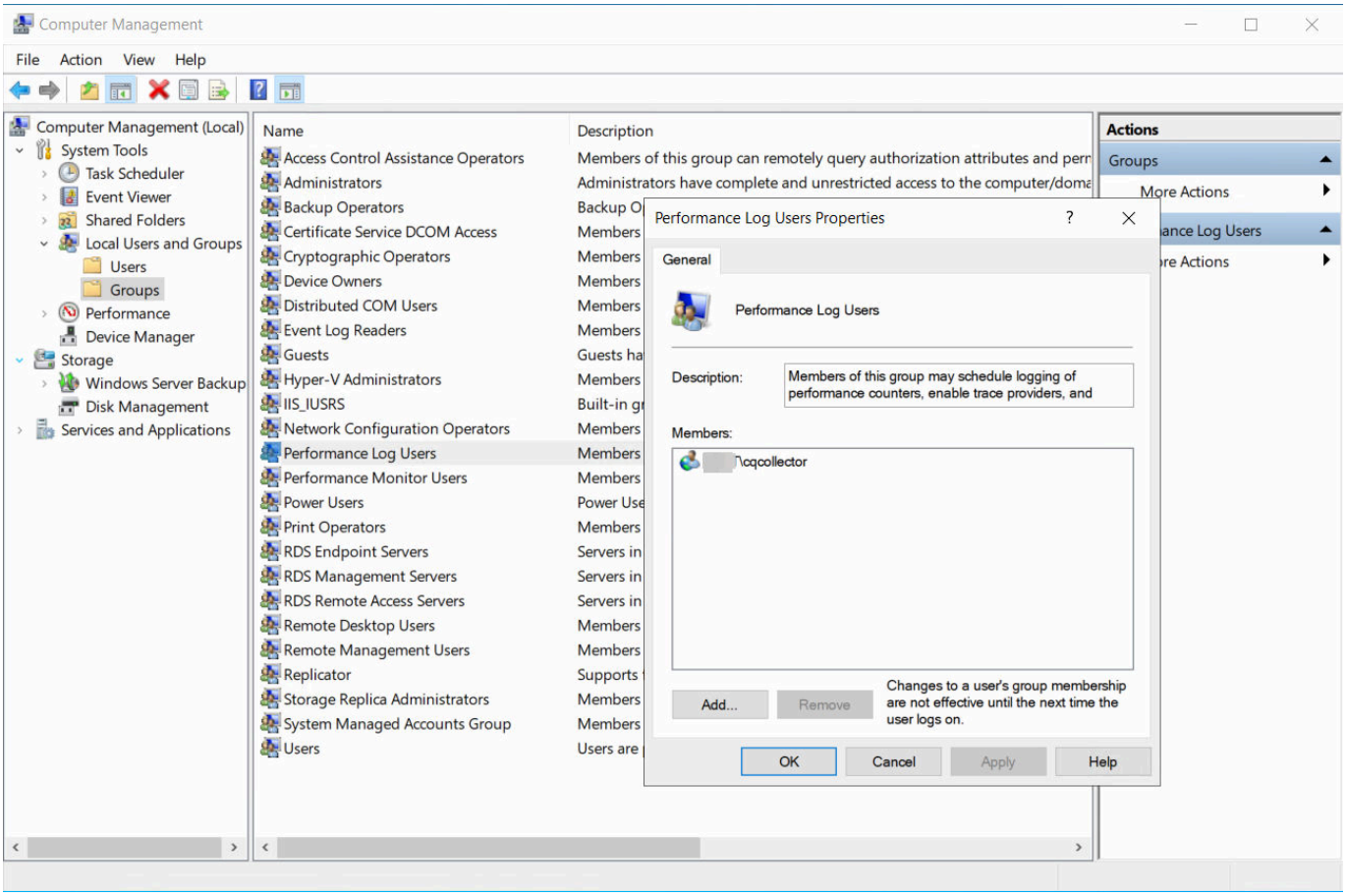
The password is encoded on a station where the CYBERUQEST Agent is installed. To encode the password, follow these steps:

1. Open a CMD window;
2. Navigate to **"C:\Program Files (x86)\CyberQuestAgent"**, where the CYBERQUEST Agent is installed.
3. Execute command **"Agent.exe -encodepassword=1234**, where "1234" is the password that should be encoded.
4. The result is a hashed password, as shown below:



Operations · VMI Permissions

Considering that this user account is already part of the “Domain Users” group, remote WMI access must be enabled to use it as a service account with restricted permissions. To achieve this, add the user account to the local “Performance Log Users” group:

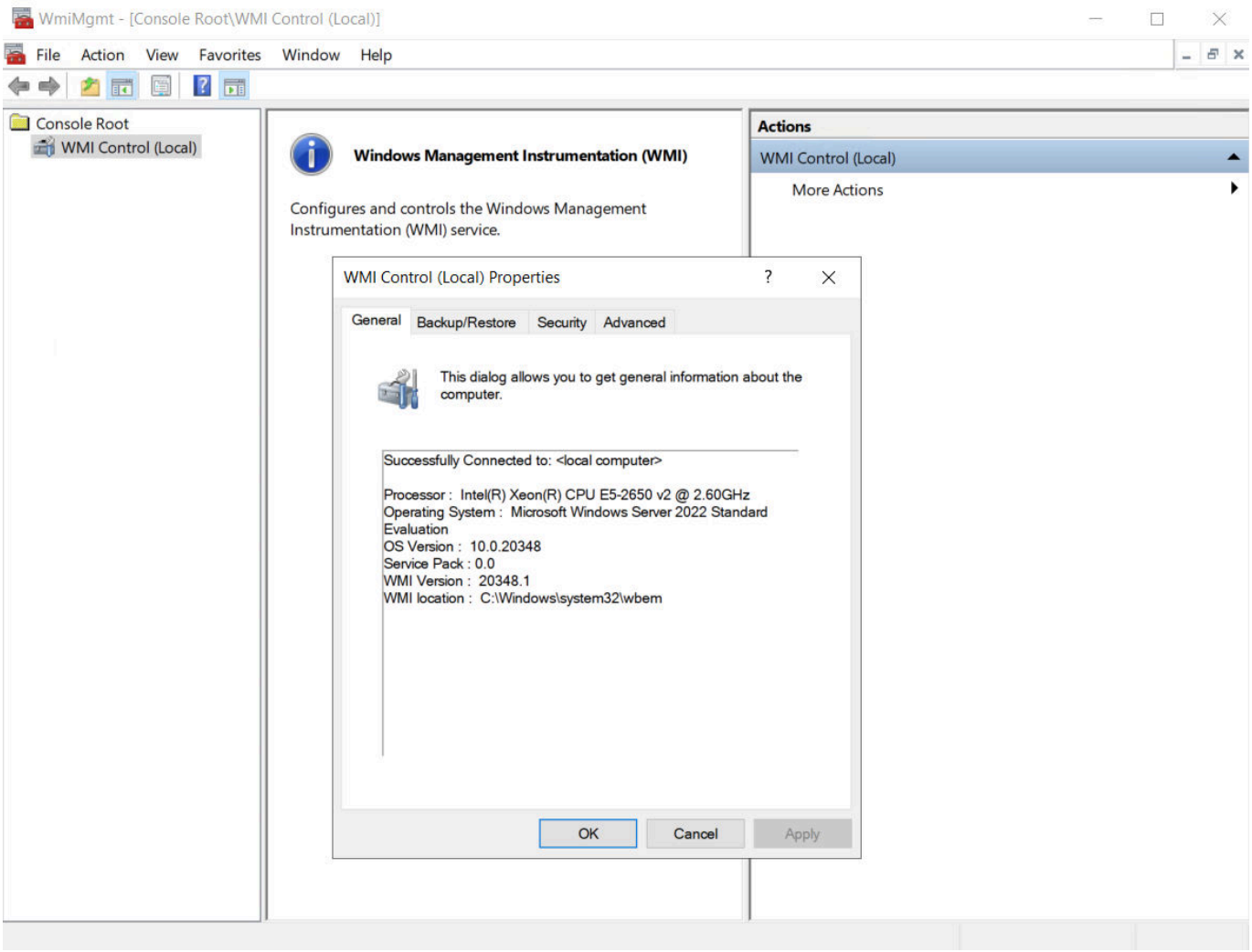


Then allow a user to have access via WMI Control Properties:

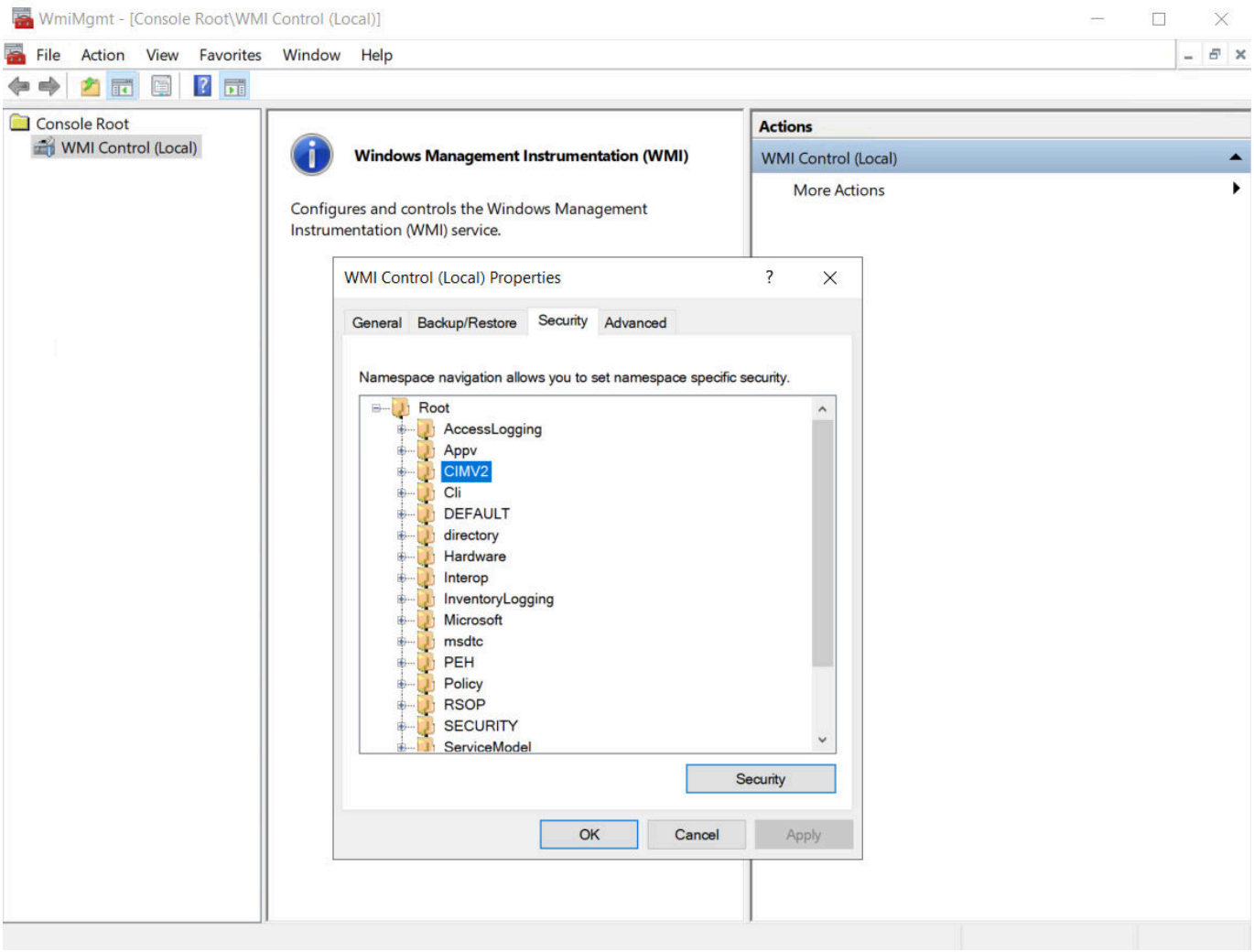
1.Open the WMI Control console: Click Start, choose Run and type wmimgmt.msc, then click OK.

2.In the console tree, right-click WMI Control and then click Properties.

3.Click the Security tab.

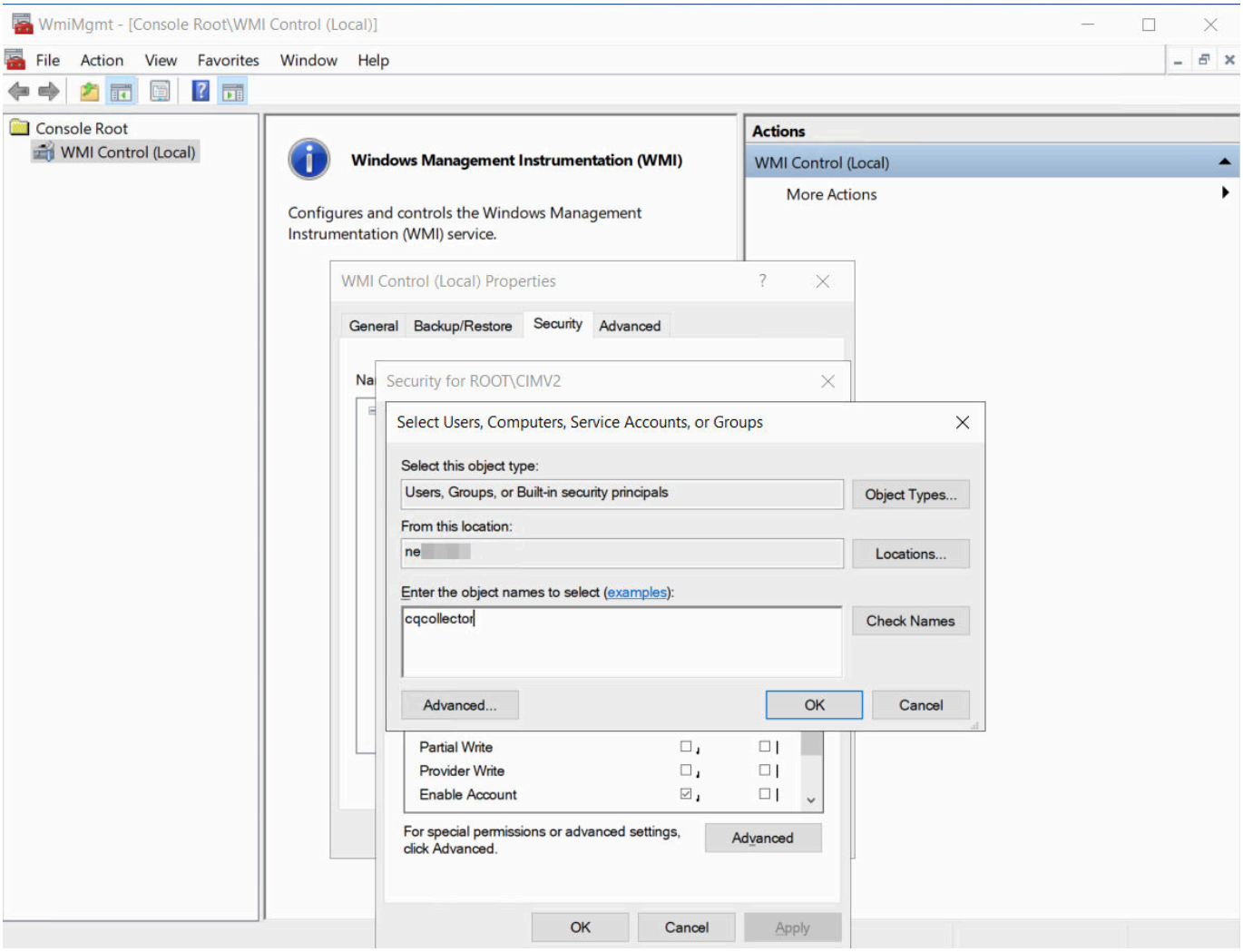


Select the "\Root\CIMV2" namespace to choose which user or group will have access, and then click on Security.

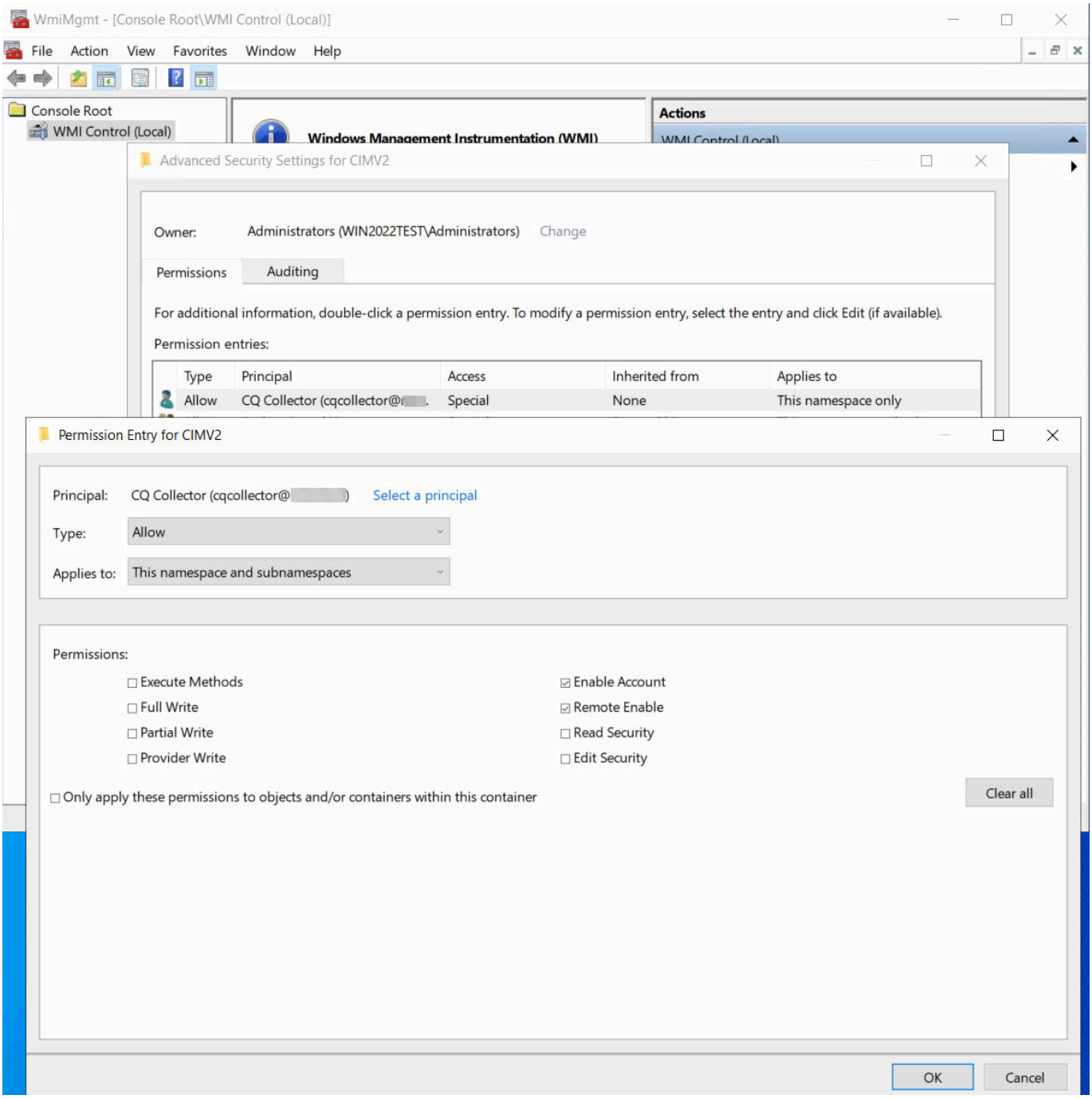


In the Security dialog box, click Add.

In the Select Users, Computers, or Groups dialog box, enter the name of the object (user or group) that you want to add, click OK and then choose Advanced.



In the Advanced Security dialog box under Permissions, edit the permissions and check the “Enable Account” and “Remote Enable” boxes. Select Apply to “This namespace and subnamespaces”:



Click OK 4 times to close all the windows.

And now you're finished! The user now has remote access to WMI information.

Operations · VMI Ports

The following ports are used for WMI queries:

- VMI Ports TCP 135, TCP 139, TCP 445 and "Remote Registry Service" and "Windows Management Instrumentation" services.

And the following port ranges:

Windows Server 2008 and later versions, and in Windows Vista and later versions, the default dynamic port range changed to the following range:

- Start port: TCP 49152
- End port: TCP 65535

Windows 2000, Windows XP, and Windows Server 2003 use the following dynamic port range:

- Start port: TCP 1025
- End port: TCP 5000

As detailed in the following article: Service overview and network port requirements for Windows (https://learn.microsoft.com/en-us/troubleshoot/windows-server/networking/service-overview-and-network-port-requirements)

Third-Party Components

Licensing

Web Applications

CYBERQUEST uses third party components for it's services, as follows:

Web Application - composer

Name of Component	License
Monolog	Monolog license (https://github.com/Seldaek/monolog/blob/2.x/LICENSE)
Slim-Psr7	Slim-Psr7 license (https://github.com/slimphp/Slim-Psr7/blob/master/LICENSE.md)
Slim	Slim license (https://github.com/slimphp/Slim/blob/4.x/LICENSE.md)
Phpunit	Phpunit license (https://packagist.org/packages/phpunit/phpunit)
GeoIP2-php	GeoIP2-php license (https://github.com/maxmind/GeoIP2-php)
Php-amqplib	Php-amqplib license (https://github.com/php-amqplib/php-amqplib/blob/master/LICENSE)
Predis	Predis license (https://github.com/predis/predis/blob/v1.1/LICENSE)
PhpSpreadsheet	PhpSpreadsheet license (https://github.com/PHPOffice/PhpSpreadsheet/blob/master/LICENSE)
PHP-DI	PHP-DI license (https://github.com/PHP-DI/PHP-DI/blob/master/LICENSE)
PHPExcel	PHPExcel license (https://github.com/PHPOffice/PHPExcel/blob/1.8/license.md)
Mpdf	Mpdf license (https://github.com/mpdf/mpdf/blob/development/LICENSE.txt)
FPDF	FPDF license (https://github.com/Setasign/FPDF/blob/master/license.txt)
FPDI	FPDI license (https://github.com/Setasign/FPDI/blob/master/LICENSE.txt)
Laravel-mcrypt-faker	Laravel-mcrypt-faker license (https://github.com/thomaswelton/laravel-mcrypt-faker)
Slim-session	Slim-session license (https://github.com/bryanjhv/slim-session/blob/master/license.txt)
FastRoute	FastRoute license (https://github.com/nikic/FastRoute/blob/master/LICENSE)
PHP-View	PHP-View license (https://github.com/slimphp/PHP-View/blob/3.x/LICENSE.md)
Guzzle	Guzzle license (https://github.com/guzzle/guzzle/blob/master/LICENSE)
Collect	Collect license (https://github.com/tighten/collect)
Validation	Validation license (https://github.com/Respect/Validation/blob/master/LICENSE)
Phpfastcache	Phpfastcache license (https://github.com/PHPSocialNetwork/phpfastcache/blob/master/LICENCE)
Laminas-mail	Laminas-mail license (https://github.com/laminas/laminas-mail/blob/2.17.x/LICENSE.md)
Laminas-crypt	Laminas-cryt license (https://github.com/laminas/laminas-crypt/blob/3.9.x/LICENSE.md)
Laminas-servicemanager	Laminas-servicemanager license (https://github.com/laminas/laminas-servicemanager/blob/3.12.x/LICENSE.md)
Php-jwt	Php-jwt license (https://github.com/firebase/php-jwt/blob/main/LICENSE)
Phpdotenv	Phpdotenv license (https://github.com/vlucas/phpdotenv/blob/master/LICENSE)
Terminal	Terminal license (https://github.com/TitasGailius/terminal)
tFPDF	tFPDF license (https://github.com/Setasign/tFPDF)
Phpunit	Phpunit license (https://github.com/sebastianbergmann/phpunit/blob/main/LICENSE)
Codeception	Codeception license (https://github.com/Codeception/Codeception/blob/5.0/LICENSE)
module-asserts	Module-asserts license (https://github.com/Codeception/module-asserts/blob/master/LICENSE)
module-phpbrowser	Module-phpbrowser license (https://github.com/Codeception/module-phpbrowser/blob/master/LICENSE)
module-webdriver	Module-webdriver license (https://github.com/Codeception/module-webdriver/blob/master/LICENSE)
module-cli	Module-cli license (https://github.com/Codeception/module-cli/blob/master/LICENSE)
GoogleAuthenticator	GoogleAuthenticator license (https://github.com/sonata-project/GoogleAuthenticator/blob/2.x/LICENSE)
php-encryption	php-encryption license (https://github.com/defuse/php-encryption/blob/master/LICENSE)
qr-code	qr-code license (https://github.com/endroid/qr-code/blob/master/LICENSE)

Name of Component	License
@fortawesome/fontawesome-pro	@fortawesome/fontawesome-pro license (https://fontawesome.com/docs/web/setup/packages)
@types/codemirror	@types/codemirror license (https://github.com/DefinitelyTyped/DefinitelyTyped/tree/master/types/codemirror)
react-icons	react-icons license (https://github.com/react-icons/react-icons/blob/master/LICENSE)
style-loader	style-loader license (https://github.com/webpack-contrib/style-loader/blob/master/LICENSE)
terser-webpack-plugin	terser-webpack-plugin license (https://github.com/webpack-contrib/terser-webpack-plugin/blob/master/LICENSE)
typescript	typescript license (https://github.com/microsoft/TypeScript/blob/main/LICENSE.txt)
webpack	webpack license (https://github.com/webpack/webpack/blob/main/LICENSE)
webpack-cli	webpack-cli license (https://github.com/webpack/webpack-cli/blob/master/LICENSE)
webpack-livereload-plugin	webpack-livereload-plugin license (https://github.com/statianzo/webpack-livereload-plugin/blob/master/LICENSE)
axios	axios license (https://github.com/axios/axios/blob/master/LICENSE)
babel-preset-react-app	babel-preset-react-app license (https://github.com/facebook/create-react-app/blob/main/LICENSE)
bootstrap	bootstrap license (https://github.com/twbs/bootstrap/blob/main/LICENSE)
bootstrap4-toggle	bootstrap4-toggle license (https://github.com/gitbrent/bootstrap4-toggle/blob/master/LICENSE)
c3	c3 license (https://github.com/c3js/c3/blob/master/LICENSE)
cities.json	cities.json license (https://github.com/lutangar/cities.json)
codemirror	codemirror license (https://github.com/codemirror/CodeMirror/blob/master/LICENSE)
collect.js	collect.js license (https://github.com/ecrmnn/collect.js/blob/master/LICENSE.md)
d3-geo-projection	d3-geo-projection license (https://github.com/d3/d3-geo-projection/blob/main/LICENSE)
d3-scale	d3-scale license (https://github.com/d3/d3-scale/blob/main/LICENSE)
datatables.net-bs4	datatables.net-bs4 license (https://github.com/DataTables/Dist-DataTables-Bootstrap4/blob/master/License.txt)
datatables.net-buttons	datatables.net-buttons license (https://github.com/DataTables/Dist-DataTables-Buttons/blob/master/License.txt)
datatables.net-colreorder-bs4	datatables.net-colreorder-bs4 license (https://github.com/DataTables/Dist-DataTables-ColReorder-Bootstrap4/blob/master/License.txt)
datatables.net-keytable-bs4	datatables.net-keytable-bs4 license (https://github.com/DataTables/Dist-DataTables-KeyTable-Bootstrap4/blob/master/License.txt)
datatables.net-responsive-bs4	datatables.net-responsive-bs4 license (https://github.com/DataTables/Dist-DataTables-Responsive-Bootstrap4/blob/master/License.txt)
datatables.net-scroller-bs4	datatables.net-scroller-bs4 license (https://github.com/DataTables/Dist-DataTables-Scroller-Bootstrap4/blob/master/License.txt)
datatables.net-select-bs4	datatables.net-select-bs4 license (https://github.com/DataTables/Dist-DataTables-Select-Bootstrap4/blob/master/License.txt)
date-fns	date-fns license (https://github.com/date-fns/date-fns/blob/master/LICENSE.md)
export-from-json	export-from-json license (https://github.com/zheeeng/export-from-json/blob/master/LICENSE)
flatpickr	flatpickr license (https://github.com/flatpickr/flatpickr/blob/master/LICENSE.md)
html2canvas	html2canvas license (https://github.com/niklasvh/html2canvas/blob/master/LICENSE)
input-moment	input-moment license (https://github.com/wangzuo/input-moment/blob/master/LICENSE)

Name of Component	License
iso-country-codes	iso-country-codes license (https://github.com/joonhocho/iso-country-codes/blob/master/LICENSE)
jquery	jquery license (https://github.com/jquery/jquery/blob/main/LICENSE.txt)
jquery-base64	jquery-base64 license (https://github.com/xuanhoa88/jquery-base64)
jQuery-QueryBuilder	jQuery-QueryBuilder license (https://github.com/mistic100/jQuery-QueryBuilder/blob/dev/LICENSE)
jquery-ui	jquery-ui license (https://github.com/jquery/jquery-ui/blob/main/LICENSE.txt)
jquery.fancytree	jquery.fancytree license (https://github.com/mar10/fancytree/blob/master/LICENSE.txt)
js-file-download	js-file-download license (https://github.com/kennethjiang/js-file-download/blob/master/LICENSE)
jshint	jshint license (https://github.com/jshint/jshint/blob/main/LICENSE)
leaflet	leaflet license (https://github.com/Leaflet/Leaflet/blob/main/LICENSE)
lodash	lodash license (https://github.com/lodash/lodash/blob/master/LICENSE)
lucene	lucene license (https://github.com/bripkens/lucene/blob/master/LICENSE)
moment	moment license (https://github.com/moment/moment/blob/develop/LICENSE)
path	path license (https://github.com/jinder/path/blob/master/LICENSE)
popper	popper license (https://github.com/pemrouz/popper)
quill	quill license (https://github.com/quilljs/quill)
rc-tree	rc-tree license (https://github.com/react-component/tree/blob/master/LICENSE.md)
react	react license (https://github.com/facebook/react/blob/main/LICENSE)
react-accessible-accordion	react-accessible-accordion license (https://github.com/springload/react-accessible-accordion/blob/main/LICENSE)
react-base-table	react-base-table license (https://github.com/Autodesk/react-base-table/blob/master/LICENSE.md)
react-bootstrap	react-bootstrap license (https://github.com/react-bootstrap/react-bootstrap/blob/master/LICENSE)
react-bootstrap-modal	react-bootstrap-modal license (https://github.com/jquense/react-bootstrap-modal/blob/master/License.txt)
react-bootstrap-slider	react-bootstrap-slider license (https://github.com/browniebroy/react-bootstrap-slider/blob/master/README.md)
react-bootstrap-table	react-bootstrap-table license (https://github.com/AllenFang/react-bootstrap-table/blob/master/LICENSE)
react-bootstrap-toggle	react-bootstrap-toggle license (https://github.com/arnthor3/react-bootstrap-toggle/blob/master/LICENSE)
react-circular-progressbar	react-circular-progressbar license (https://github.com/kevinsqi/react-circular-progressbar/blob/master/LICENSE)
react-codemirror2	react-codemirror2 license (https://github.com/scniro/react-codemirror2)
react-container-dimensions	react-container-dimensions license (https://github.com/okonet/react-container-dimensions/blob/master/LICENSE)
react-csv	react-csv license (https://github.com/react-csv/react-csv/blob/master/LICENSE.txt)
react-data-table-component	react-data-table-component license (https://github.com/jbetancur/react-data-table-component/blob/master/LICENSE)
react-datamaps	react-datamaps license (https://github.com/btmills/react-datamaps/blob/master/LICENSE)
react-datamaps	react-datamaps license (https://github.com/btmills/react-datamaps/blob/master/LICENSE)
react-datepicker	react-datepicker license (https://github.com/Hacker0x01/react-datepicker/blob/master/LICENSE)
react-datetime	react-datetime license (https://github.com/arqex/react-datetime/blob/master/README.md)

Name of Component	License
react-dnd	react-dnd license (https://github.com/react-dnd/react-dnd/blob/main/LICENSE)
react-dnd-html5-backend	react-dnd-html5-backend license (https://github.com/react-dnd/react-dnd/blob/main/LICENSE)
react-dom	react-dom license (https://github.com/facebook/react/blob/main/LICENSE)
react-dom-inject	react-dom-inject license (https://github.com/noderaider/react-dom-inject/blob/master/LICENSE)
react-flags	react-flags license (https://github.com/wiredmax/react-flags/blob/master/LICENSE)
react-flatpickr	react-flatpickr license (https://github.com/haoxins/react-flatpickr/blob/master/LICENSE)
react-leaflet	react-leaflet license (https://github.com/PaulLeCam/react-leaflet/blob/master/LICENSE.md)
react-motion	react-motion license (https://github.com/chenglou/react-motion)
react-overlays	react-overlays license (https://github.com/react-bootstrap/react-overlays/blob/master/LICENSE)
react-qr-code	react-qr-code license (https://github.com/rosskhanas/react-qr-code/blob/master/LICENSE)
react-querybuilder	react-querybuilder license (https://github.com/react-querybuilder/react-querybuilder/blob/main/LICENSE.md)
react-quill	react-quill license (https://github.com/zenoamaro/react-quill/blob/master/LICENSE)
react-redux	react-redux license (https://github.com/reduxjs/react-redux/blob/master/LICENSE.md)
react-router-dom	react-router-dom license (https://github.com/remix-run/react-router)
react-select	react-select license (https://github.com/JedWatson/react-select/tree/master/packages/react-select)
react-simple-maps	react-simple-maps license (https://github.com/zcreativelabs/react-simple-maps/blob/master/LICENSE)
react-slider	react-slider license (https://github.com/zillow/react-slider/blob/master/LICENSE)
react-sortable-hoc	react-sortable-hoc license (https://github.com/clauderic/react-sortable-hoc/blob/master/LICENSE)
react-spinners	react-spinners license (https://github.com/davidhu2000/react-spinners/blob/main/LICENSE)
react-tooltip	react-tooltip license (https://github.com/wwayne/react-tooltip/blob/master/LICENSE)
recharts	recharts license (https://github.com/recharts/recharts/blob/master/LICENSE)
simple-react-validator	simple-react-validator license (https://github.com/dockwa/simple-react-validator/blob/master/License)
socket.io	socket.io license (https://github.com/socketio/socket.io/blob/main/LICENSE)
styled-components	styled-components license (https://github.com/styled-components/styled-components/blob/main/LICENSE)
sweetalert2	sweetalert2 license (https://github.com/sweetalert2/sweetalert2/blob/main/LICENSE)
tempusdominus-core	tempusdominus-core license (https://github.com/tempusdominus/core/blob/master/LICENSE)
topojson-client	topojson-client license (https://github.com/topojson/topojson-client/blob/master/LICENSE)
typeahead	typeahead license (https://github.com/defunctzombie/typeahead/blob/master/LICENSE)
uikit	uikit license (https://github.com/uikit/uikit/blob/develop/LICENSE.md)
update	update license (https://github.com/update/update/blob/master/LICENSE)
use-bus	use-bus license (https://github.com/fabienjuif/use-bus/blob/master/LICENSE)
use-interval	use-interval license (https://github.com/Hermanya/use-interval/blob/master/LICENSE)
utf8	utf8 license (https://github.com/mathiasbynens/utf8.js/blob/master/LICENSE-MIT.txt)
webpack-jquery-ui	webpack-jquery-ui license (https://www.npmjs.com/package/webpack-jquery-ui)

Data Acquisition and Data Server

Data Acquistion & Data Correlation & Data Server

Name of Component	License
Curl	Copyright license (https://curl.se/docs/copyright.html)
libmaxminddb	libmaxminddb license (https://github.com/maxmind/libmaxminddb/blob/main/LICENSE)
rabbitmq-c	rabbitmq-c license (https://github.com/alanxz/rabbitmq-c/blob/master/LICENSE)
Zlib	Zlib license (https://opensource.org/licenses/Zlib)
v8/v8.git/+/master	v8/v8.git/+/master license (https://chromium.googlesource.com/v8/v8.git/+/master/LICENSE)
hiredis	hiredis license (https://github.com/redis/hiredis/blob/master/COPYING)
pcrexx	pcrexx license (https://github.com/AndreLouisCaron/pcrexx/blob/master/LICENSE.txt)
PCRE	PCRE license (https://www.pcre.org/original/license.txt)
mariadb-connector-c	mariadb-connector-c license (https://github.com/StableCoder/mariadb-connector-c/blob/master/LICENSE)

Data Storage

Name of Component	License
Apache log4j	Apache log4j license (https://logging.apache.org/log4j/2.x/license.html)
commons-bsf	commons-bsf license (https://commons.apache.org/proper/commons-bsf/license.html)
netty	netty license (https://github.com/netty/netty/blob/4.1/LICENSE.txt)
gson	gson license (https://github.com/google/gson/blob/master/LICENSE)
commons-configuration	commons-configuration license (https://github.com/apache/commons-configuration/blob/master/LICENSE.txt)
commons-beanutils	commons-beanutils license (https://github.com/apache/commons-beanutils/blob/master/LICENSE.txt)
rabbitmq	rabbitmq license (https://www.rabbitmq.com/mpl.html)
common-logging	common-logging license (https://github.com/net-commons/common-logging/blob/master/license.txt)
commons-io	commons-io license (https://github.com/apache/commons-io/blob/master/LICENSE.txt)
bouncycastle	bouncycastle license (https://www.bouncycastle.org/license.html)
commons-dbutils	commons-dbutils license (https://github.com/apache/commons-dbutils/blob/master/LICENSE.txt)
MySQL Connector/J 8.0	MySQL Connector/J 8.0 license (https://downloads.mysql.com/docs/licenses/connector-j-8.0-gpl-en.pdf)
commons-daemon	commons-daemon license (https://commons.apache.org/proper/commons-daemon/)
jdeb	jdeb license (https://mvnrepository.com/artifact/org.vafer/jdeb)
Apache	Apache license (https://hc.apache.org/licenses.html)
junit5	junit5 license (https://github.com/junit-team/junit5/blob/main/LICENSE.md)
maven-project-info-reports-plugin	maven-project-info-reports-plugin license (https://maven.apache.org/plugins/maven-project-info-reports-plugin/licenses-mojo.html)
plugins-archives	plugins-archives license (https://maven.apache.org/plugins-archives/maven-assembly-plugin-2.4.1/license.html)

Windows Agent

Name of Component	License
AdvancedStringBuilder	AdvancedStringBuilder license (https://github.com/Taritsyn/AdvancedStringBuilder/blob/master/LICENSE.txt)
bouncycastle	bouncycastle license (https://www.bouncycastle.org/license.html)
protobuf	protobuf license (https://github.com/protocolbuffers/protobuf/blob/main/LICENSE)
IpMatcher	IpMatcher license (https://github.com/jchristn/IpMatcher/blob/master/LICENSE.md)
K4os.Compression.LZ4	K4os.Compression.LZ4 license (https://github.com/MiloszKrajewski/K4os.Compression.LZ4/blob/master/LICENSE)
license-k4os-compression-lz4-streams	license-k4os-compression-lz4-streams (https://docs.oracle.com/cd/E17952_01/connector-net-8.0-license-gpl-en/license-k4os-compression-lz4-streams.html)
K4os.Hash.xxHash	K4os.Hash.xxHash license (https://github.com/MiloszKrajewski/K4os.Hash.xxHash/blob/master/LICENSE)
MIT	MIT license (https://licenses.nuget.org/MIT)
ClearScript	ClearScript license (https://github.com/microsoft/ClearScript/blob/master/License.txt)
Microsoft.ClearScript.Core	Microsoft.ClearScript.Core license (https://www.nuget.org/packages/Microsoft.ClearScript.Core/7.2.4/License)
Microsoft.ClearScript.V8	Microsoft.ClearScript.V8 license (https://www.nuget.org/packages/Microsoft.ClearScript.V8/)
Microsoft.ClearScript.V8.ICUData	Microsoft.ClearScript.V8.ICUData license (https://www.nuget.org/packages/Microsoft.ClearScript.V8.ICUData/)
Microsoft.ClearScript.V8.Native.win-x64	Microsoft.ClearScript.V8.Native.win-x64 license (https://www.nuget.org/packages/Microsoft.ClearScript.V8.Native.win-x64/)
Microsoft.ClearScript.V8.Native.win-x86	Microsoft.ClearScript.V8.Native.win-x86 license (https://www.nuget.org/packages/Microsoft.ClearScript.V8.Native.win-x86/)
Microsoft.ClearScript.Windows Namespace	Microsoft.ClearScript.Windows Namespace license (https://microsoft.github.io/ClearScript/Reference/html/N_Microsoft_ClearScript_Windows.htm)
Newtonsoft.Json	Newtonsoft.Json license (https://github.com/JamesNK/Newtonsoft.Json/blob/master/LICENSE.md)
Npgsql - .NET Access to PostgreSQL	Npgsql - .NET Access to PostgreSQL license (https://www.npgsql.org/#license)
.NET/C# RabbitMQ Client Library	.NET/C# RabbitMQ Client Library license (https://www.rabbitmq.com/dotnet.html)
System.Text.Encodings.Web	System.Text.Encodings.Web license (https://www.nuget.org/packages/System.Text.Encodings.Web)
System.Text.Json	System.Text.Json license (https://www.nuget.org/packages/System.Text.Json)
System.ValueTuple	System.ValueTuple license (https://www.nuget.org/packages/System.ValueTuple/)
watson-online-store	watson-online-store license (https://github.com/IBM/watson-online-store/blob/master/LICENSE)
routing	routing license (https://github.com/symfony/Routing/blob/5.4/Matcher/UrlMatcher.php)
log4net	log4net license (https://logging.apache.org/log4net/license.html)
Microsoft.Diagnostics.Tracing.EventSource.Redist	Microsoft.Diagnostics.Tracing.EventSource.Redist license (https://www.nuget.org/packages/Microsoft.Diagnostics.Tracing.EventSource.Redist/)
mysql-data-api	mysql-data-api license (https://github.com/Fyreware/mysql-data-api/blob/dev/LICENSE.md)
Net.Code.Csv	Net.Code.Csv license (https://www.nuget.org/packages/Net.Code.Csv/)
NUnit	NUnit license (https://nunit.org/)

Name of Component	License
Oracle.ManagedDataAccess	Oracle.ManagedDataAccess license (https://www.nuget.org/packages/Oracle.ManagedDataAccess/)
RegexMatcher	RegexMatcher license (https://github.com/jchristn/RegexMatcher/blob/master/LICENSE.md)
RoboSharp	RoboSharp license (https://github.com/tjscience/RoboSharp/blob/dev/license)
SSH.NET	SSH.NET license (https://github.com/sshnet/SSH.NET/blob/develop/LICENSE)
System.Buffers	System.Buffers license (https://www.nuget.org/packages/System.Buffers/)
System.Memory	System.Memory license (https://www.nuget.org/packages/System.Memory/)
System.Numerics.Vectors	System.Numerics.Vectors license (https://www.nuget.org/packages/System.Numerics.Vectors/)
System.Runtime.CompilerServices.Unsafe	System.Runtime.CompilerServices.Unsafe license (https://www.nuget.org/packages/System.Runtime.CompilerServices.Unsafe/)
System.Threading.Channels	System.Threading.Channels license (https://www.nuget.org/packages/System.Threading.Channels/)
System.Threading.Tasks.Extensions	System.Threading.Tasks.Extensions license (https://www.nuget.org/packages/System.Threading.Tasks.Extensions/)
wix	wix license (https://www.nuget.org/packages/wix/4.0.0-preview.0)
WmiLight	WmiLight license (https://www.nuget.org/packages/WmiLight/)

CyberQuest uses own modified OS for operations based on:

Base OS

Name of Component	License
Debian	Debian OS license (https://www.debian.org/legal/licenses/)
Ubuntu	Ubuntu OS license (https://ubuntu.com/legal/open-source-licences)

Additional reading

Using Regular Expressions

A regular expression (regex or regexp for short) is a special text string for describing a search pattern. There are many software applications and programming languages that support regular expressions. You can often accomplish with a single regular expression in one or a few lines of code what would otherwise take dozens or hundreds.

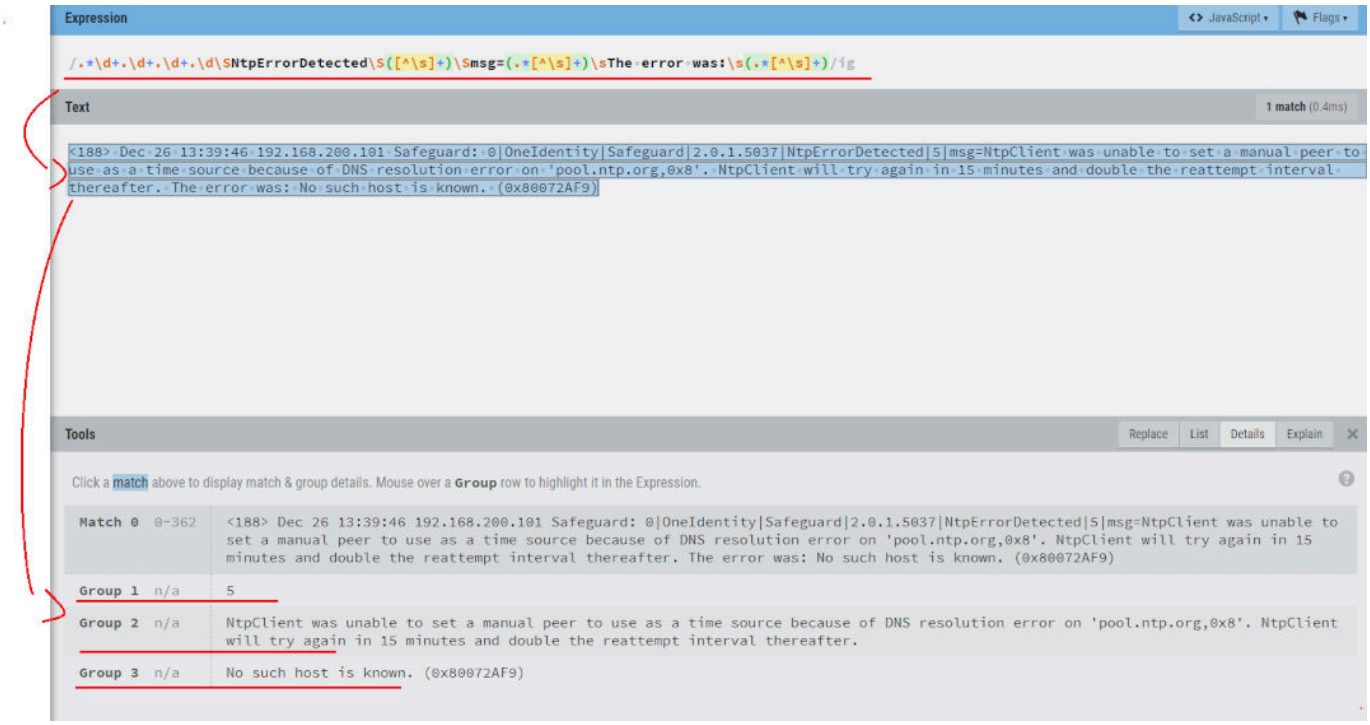
Many applications and programming languages have their own implementation of regular expressions, often with slight and sometimes with significant differences from other implementations. When two applications use a different implementation of regular expressions, we say that they use different “regular expression flavors”.

CYBERQUEST uses standard regular expressions syntax and dictionary that you can find very well described **here** (https://www.regular-expressions.info/).

You will need regular expressions to build custom parsers for various data sources you may have to accommodate for collection. This short appendix guides you to the process of creating a custom data source (parser).

Step 1: The regex

Once you have the message, you can use the help of a regular expression to extract useful information as seen below:



Step 2: The parser

After creating and testing the regular expression, go to **Settings > Rules > DTS Objects** page and create a new JS parser (DTS object) based on the earlier regex:

Name

Safeguard_parser

Description

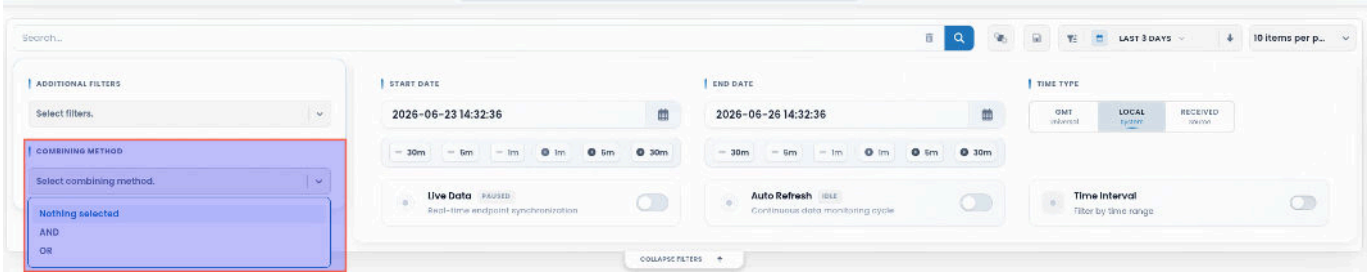
Safeguard_parser

Script

```
336       if (execResults[8] !== undefined) copyOfInputEvent.S18 = execResults[8];
337       if (execResults[9] !== undefined) copyOfInputEvent.S19 = execResults[9];
338       if (execResults[10] !== undefined) copyOfInputEvent.S20 = execResults[10];
339        copyOfInputEvent.Category = 'AccessRequestExpired';
340        copyOfInputEvent.UserName = execResults[14];
341        copyOfInputEvent.EventID = '826016';
342
343       this.outputEvents.push(copyOfInputEvent);
344      }
345     //NtpErrorDetected EventID:826017
346
347      else if (copyOfInputEvent.Description.indexOf('NtpErrorDetected') > -1) {
348
349       regex = /.*\d+.\d+.\d+.\d\SNtpErrorDetected\S([^\s]+)\Smsg=(.*[^\s]+)\sThe error was:\s(.*[^\s]+)/g;
350       execResults = regex.exec(copyOfInputEvent.Description);
351         //ConsoleLog(execResults);
352       if (execResults[1] !== undefined) copyOfInputEvent.S11 = execResults[1];
353       if (execResults[2] !== undefined) copyOfInputEvent.S22 = execResults[2];
354       if (execResults[3] !== undefined) copyOfInputEvent.S23 = execResults[3];
355
356        copyOfInputEvent.Category = 'NtpErrorDetected';
357        copyOfInputEvent.EventID = '826017';
358
359       this.outputEvents.push(copyOfInputEvent);
360      }
361    //DirectorySyncSucceeded EventID:826018
362
363      else if (copyOfInputEvent.Description.indexOf('DirectorySyncSucceeded') > -1) {
364
365       regex = /.*\d+.\d+.\d+.\d\SDirectorySyncSucceeded\S([^\s]+)\Scs1=([^\s]+)\scn1=([^\s]+)/g;
366       execResults = regex.exec(copyOfInputEvent.Description);
367         //ConsoleLog(execResults);
368       if (execResults[1] !== undefined) copyOfInputEvent.S11 = execResults[1];
369       if (execResults[2] !== undefined) copyOfInputEvent.S24 = execResults[2];
370       if (execResults[3] !== undefined) copyOfInputEvent.S25 = execResults[3];
```

Step 3: View event

Once you have the new parser, accommodate the proper filter rules and data acquisition rules as detailed in chapter Data flow rules and filters. Filters after keywords or expressions using the logical operators AND, OR, NOT:



Additional filters and combining method are available in the vertical tabs (Additional filters) and (Combining method):



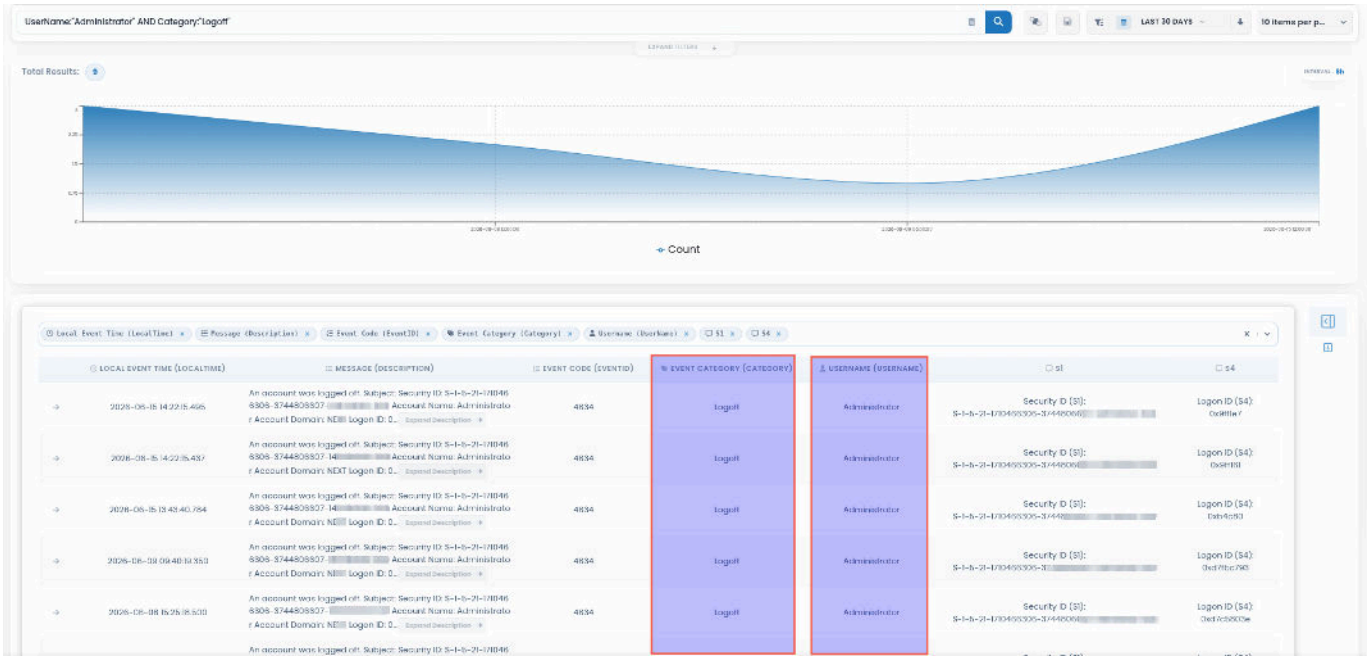
Useful information will be placed in the **S1, S2... Sn** fields.

Logical comparators and their use

Additional filters, simple or complex, can be added by using logical operators AND, OR and NOT. For example, in a search that results from only certain users and a category (ex: Logoff), a complex filter can be created like the following examples.

1. **Logical AND (&&)**

```
UserName:"Administrator" AND Category:"Logoff"
```

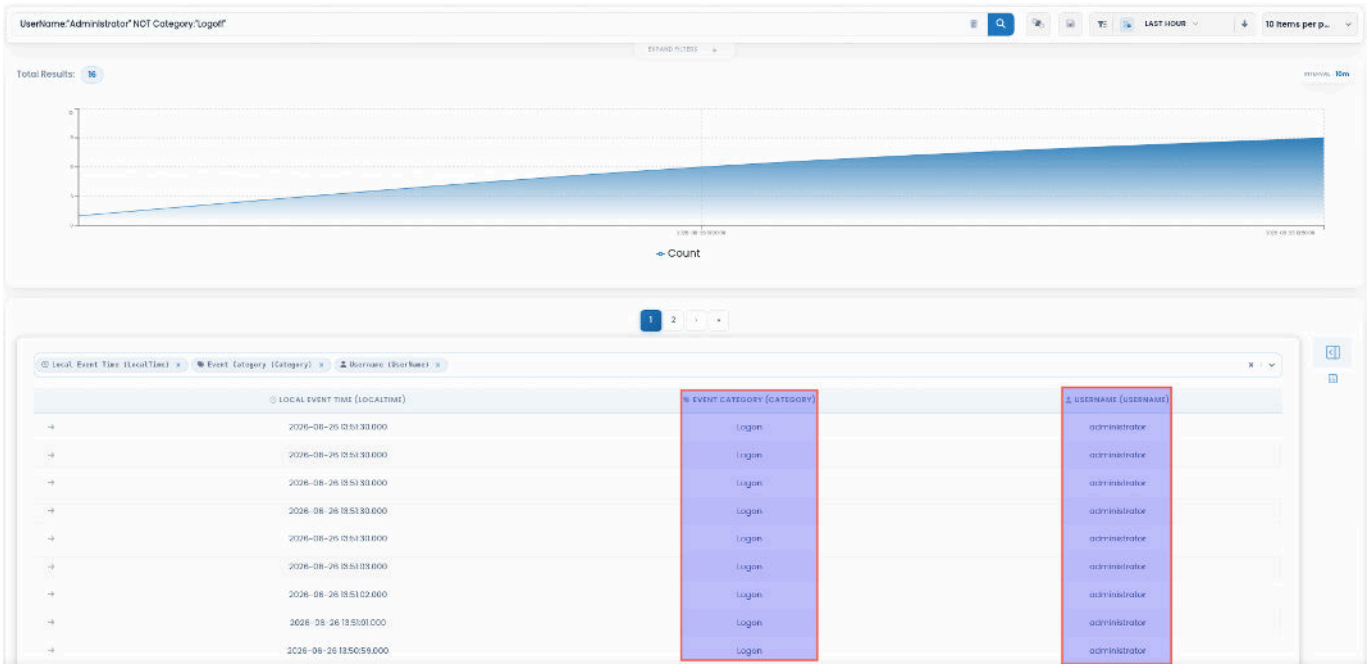


As shown, on **UserName** appears “Administrator” and on **Category** appears “Logoff”.

2. **Logical NOT (!)**

```
UserName:"Administrator" NOT Category:"Logoff"
```

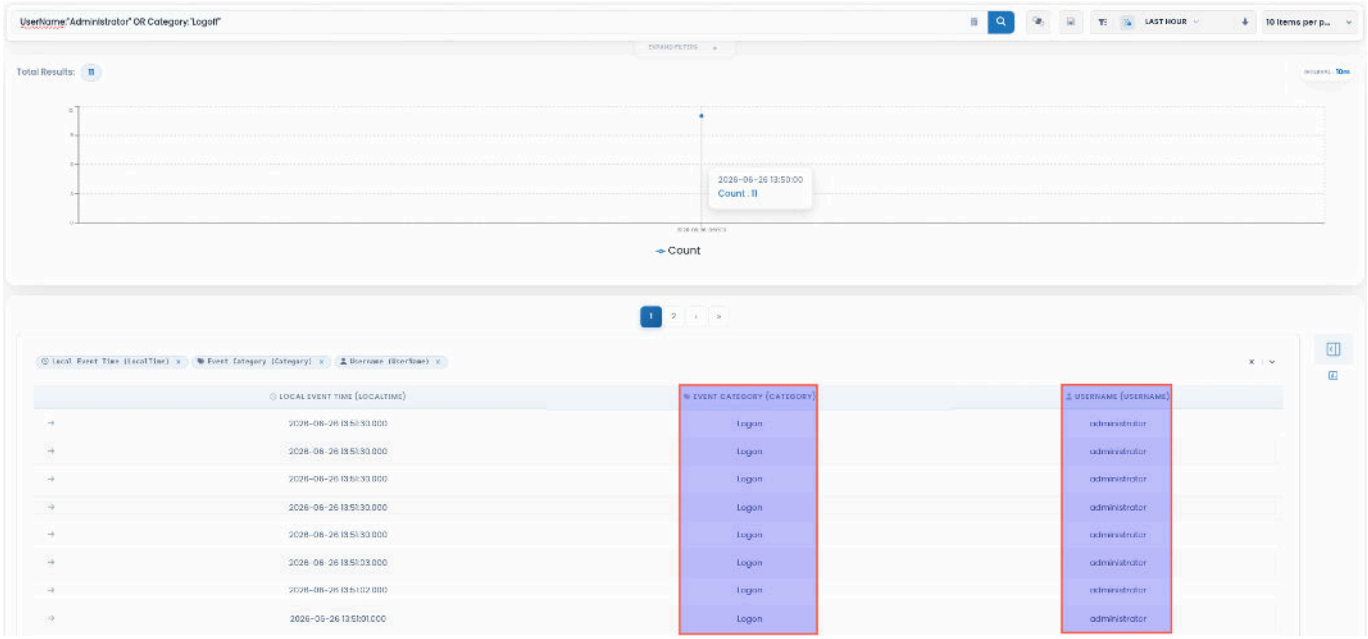
Also, in the case that you are searching for a user event that doesn't include the **Log Off** category, a complex filter can be created like this:



As shown, on **UserName** appears "Administrator" and on **Category** does not appear "Logoff".

3. **Logical OR (||)**

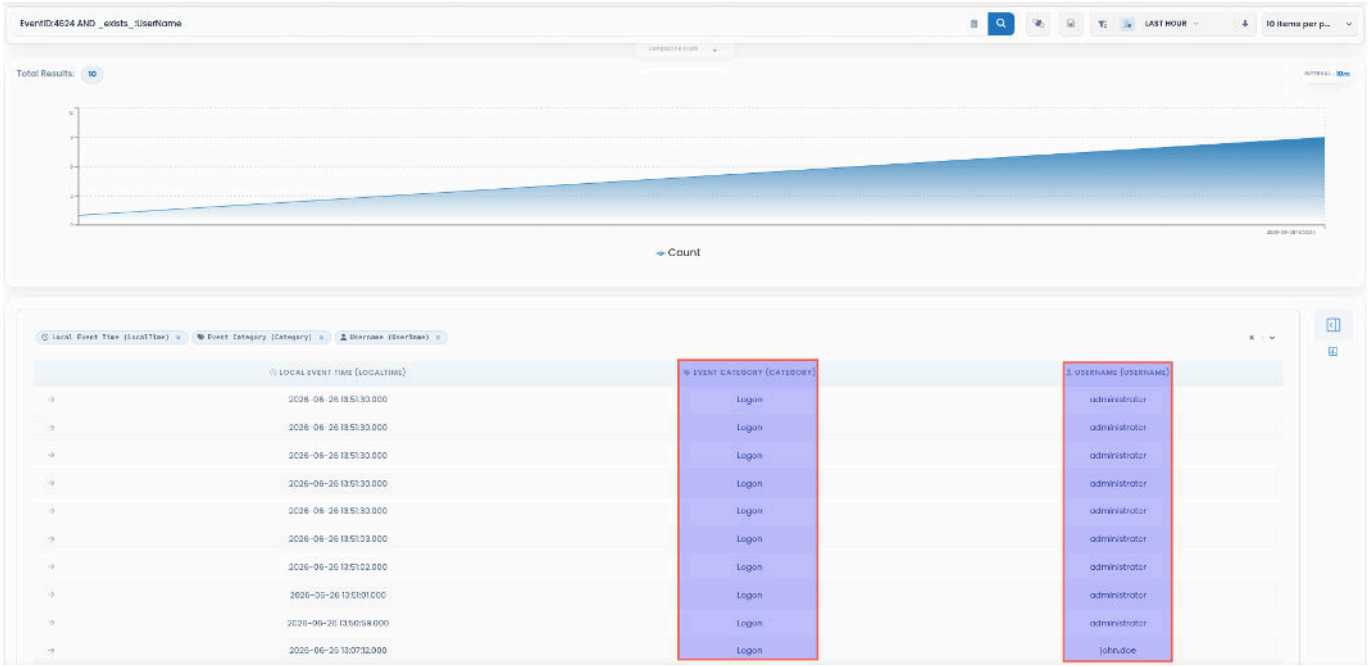
```
UserName:"Administrator" OR Category:"Logoff"
```



As shown, on **UserName** appears "Administrator" and on **Category** appears "Logoff".

4. **_exists_**

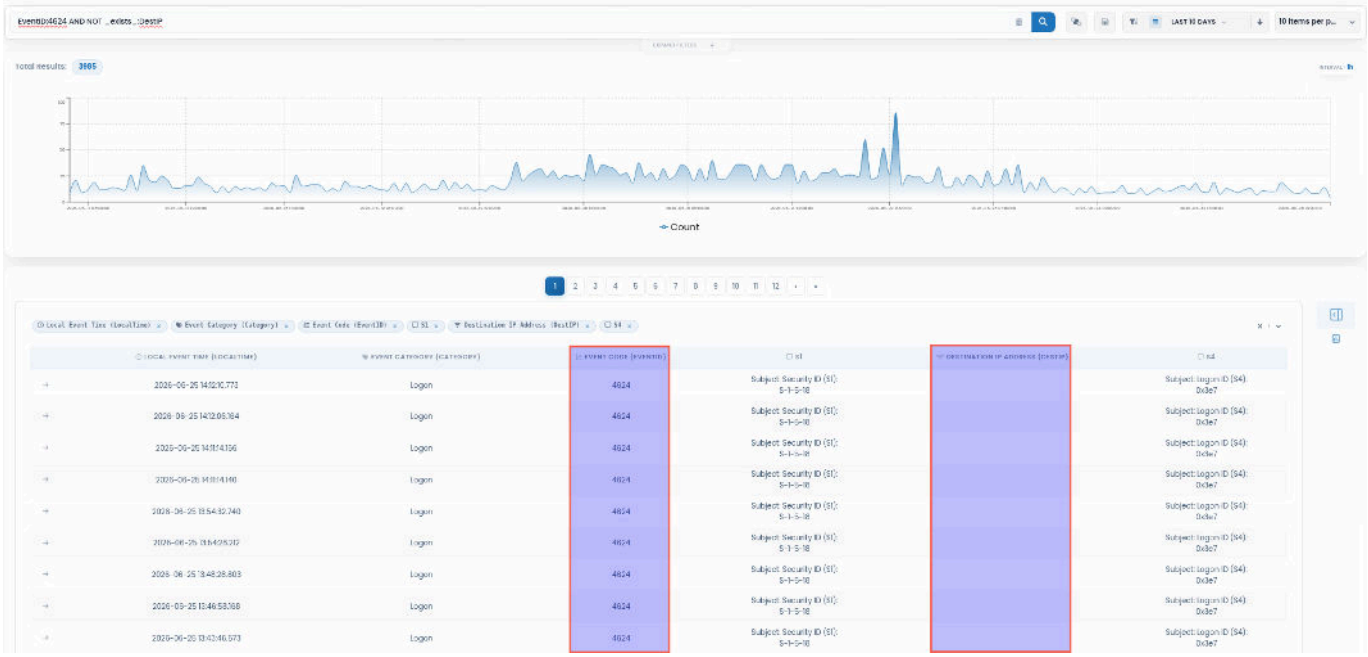
```
EventID:4624 AND _exists_:UserName
```



As shown, appears **EventID:4624** and **UserName**.

5. **NOT _exists_**

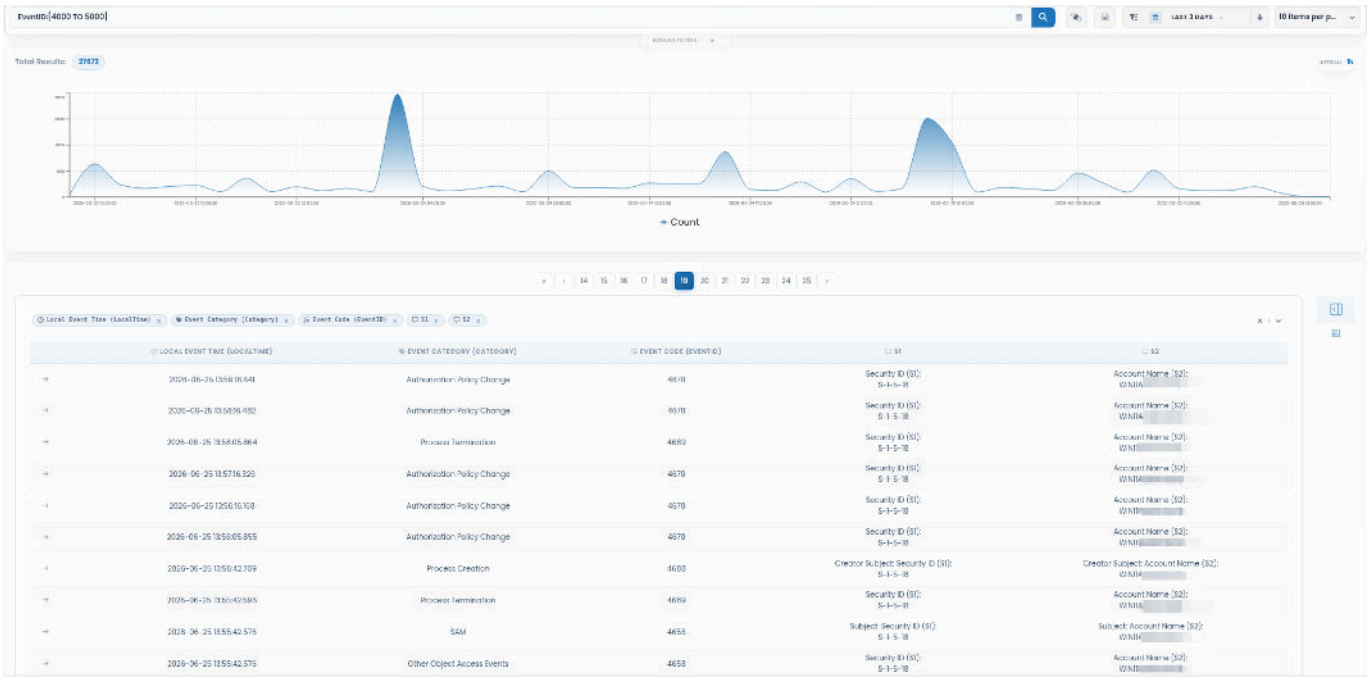
```
EventID:4624 AND _missing_:DestIP
```



As shown, appears **EventID:4624** but not **DestIP**.

6. **X TO Y**

```
EventID:[4000 TO 5000]
```



As shown, appears starting with **4000, 4001 ... and ending with 5000**.

Smart Objects

CQ Smart Objects

CYBERQUEST Smart Objects

Description

CYBERQUEST's Web Interface includes the administrative section needed for a visual configuration of your audit system.

In the log collection process, CYBERQUEST generates events in certain situations of interest to enhance the investigative process or to read information from native log source. These generated events are composed of information from one or more data streams.

Smart Objects are configured in the web interface under **Settings > Application Settings > Smart Objects**.

Each scenario below describes a specific Smart Object, including its purpose, event ID, prerequisites, history retention window, and the configuration key used to enable or disable it.

Use cases

- **Scenario 1 - *Windows Success Interactive Logon Activity***
  - Purpose - to identify, in Microsoft Windows environment, a new interactive login of a user on a station other than those in the login history.
  - Description - EventID: 9150001, a new event is generated containing details of the user and the new station on which he has interactively logged in. It also contains historical information about the stations to which he logged in interactively (MS Windows EventID 4624, logon type 2).
  - Prerequisites - Windows Security Auditing.
  - History retention of previous events - 30 days.
  - **On/Off** - *SmartObjects_WindowsSuccessInteractiveLogonActivity*
- **Scenario 2 - *Windows Success Network Logon Activity***
  - Purpose - to identify, in Microsoft Windows environment, a new network login compared to the historical ones (connection to a shared folder on a computer from the network).
  - Description - EventID: 9150002, a new event is generated containing details of the user and the network IP on which he logged in. It also contains historical information about the network resources he logged on to (MS Windows EventID 4624, logon type 3). Authentication can be done in at least 2 ways: *interactive (the station sends the authentication request to Active Directory) or based on an access to a shared resource on the network*.
  - Prerequisites - Windows Security Auditing.
  - History retention of previously events - 30 days.
  - **On/Off** - *SmartObjects_WindowsSuccessNetworkLogonActivity*
- **Scenario 3 - *Windows Success Batch Logon Activity***
  - Purpose - to identify, in Microsoft Windows environment, a new batch logon against those in history (*for example, a scheduled task*).
  - Description - EventID: 9150003, a new event is generated containing details of the user and the network IP on which he logged in. It also contains historical information about previous batch logins (MS Windows EventID 4624, logon type 4).
  - Prerequisites - Windows Security Auditing.

- History retention of previously events - 30 days.
- **On/Off** - *SmartObjects_WindowsSuccessBatchLogonActivity*

- **Scenario 4 - *Windows Success Service Logon Activity***
  - Purpose - to identify, in Microsoft Windows environment, a new service logon compared to the historical ones (*e.g. Service startup*).
  - Description - EventID: 9150004, a new event is generated containing details of the service and the IP in the network that was logged in. It also contains historical information about previous logins (MS Windows EventID 4624, logon type 5).
  - Prerequisites - Windows Security Auditing.
  - History retention of previously events - 1 year.
  - **On/Off** - *SmartObjects_WindowsSuccessServiceLogonActivity*

- **Scenario 5 - *Windows Success Network Cleartext Logon Activity***
  - Purpose - to identify, in Microsoft Windows environment, a new Cleartext authentication type compared to the historical one (where the password is transmitted in clear. Logon with credentials sent in the clear text. Most often indicates a logon to IIS with “basic authentication”).
  - Description - EventID: 9150005, a new event is generated containing details of the user and the IP in the network to which he logged in. It also contains historical information about previous logins (MS Windows EventID 4624, logon type 8).
  - Prerequisites - Windows Security Auditing.
  - History retention of previously events - 30 days.
  - **On/Off** - *SmartObjects_WindowsSuccessNetworkCleartextLogonActivity*

- **Scenario 6 ** **- *Windows Success Remote Interactive Logon Activity***
  - Purpose - to identify, in Microsoft Windows environment, a new remote interactive login in addition to the ones in the history (*Terminal Services, Remote Desktop or Remote Assistance*).
  - Description - EventID: 9150006, a new event is generated containing details of the user and network IP that logged in. It also contains historical information about previous logins (MS Windows EventID 4624, logon type 10).
  - Prerequisites - Windows Security Auditing.
  - History retention of previously events - 30 days.
  - **On/Off** - *SmartObjects_WindowsSuccessRemoteInteractiveLogonActivity*

- **Scenario 7 - *Windows Success Cached Interactive Logon Activity***
  - Purpose - to identify, in Microsoft Windows environment, a cached login after a break period of at least 3 months.
  - Description - EventID: 9150007, a new event is generated containing details of the user and network IP that logged in. It also contains historical information about previous logins (MS Windows EventID 4624, logon type 11).
  - Prerequisites - Windows Security Auditing.
  - History retention of previously events - 30 days.
  - **On/Off** - *SmartObjects_WindowsSuccessCachedInteractiveLogonActivity*

- **Scenario 8 - *Windows Failed Interactive Logon Activity***
  - Purpose - to identify, in Microsoft Windows environment, a failed interactive authentication on a station other than those in the history (user key/keyboard password).
  - Description - EventID: 9150011, a new event is generated containing details of the user and IP in the network that was logged in. It also contains historical information about previous logins (MS Windows EventID 4625, logon type 2).
  - Prerequisites - Windows Security Auditing.
  - History retention of previously events - 30 days.
  - **On/Off** - *SmartObjects_WindowsFailedInteractiveLogonActivity*

- **Scenario 9 - *Windows Failed Network Logon Activity***
  - Purpose - to identify, in Microsoft Windows environment, a new failed network authentication against the historical one (connection to a shared folder on a computer from the network).

- Description - EventID: 9150012, a new event is generated containing details of the user and IP from the network that was logged in. It also contains historical information about previous logins (MS Windows EventID 4625, logon type 3).
- Prerequisites - Windows Security Auditing.
- History retention of previously events - 30 days.
- **On/Off** - *SmartObjects_WindowsFailedNetworkLogonActivity*

- **Scenario 10 - *Windows Success Service Activity Service***
  - Purpose - to identify, in Microsoft Windows environment, authentications for new network services.
  - Description - EventID: 9150051, a new event is generated containing details of the machine in the network that has logged in and the new service registered (MS Windows EventID 4624, logon type 5). In this way, the traceability of the installation of new services at the organization level is obtained.
  - Prerequisites - Windows Security Auditing.
  - History retention of previously events - 1 year.
  - **On/Off** - *SmartObjects_WindowsSuccessServiceActivityService*

- **Scenario 11 - *Windows Success Service Activity Service User***
  - Purpose - to identify, in Microsoft Windows environment, new network logins versus those in the history, of type service run under a user.
  - Description - EventID: 9150052, a new event is generated containing details of the network machine logged on, the newly registered service/user combination (MS Windows EventID 4624, logon type 5). In this way the traceability of the installation of new services logged on by other users at the organisation level is obtained.
  - Prerequisites - Windows Security Auditing.
  - History retention of previously events - 1 year.
  - **On/Off** - *SmartObjects_WindowsSuccessServiceActivityServiceUser*

- **Scenario 12 - *Windows Success Service Activity Service Computer***
  - Purpose - to identify, in Microsoft Windows environment, new network logins versus those in the history, as a service running on a machine.
  - Description - EventID: 9150053, a new event is generated containing details of the networked machine that has been logged on, the newly registered service/user combination (MS Windows EventID 4624, logon type 5). In this way the traceability of the installation of new services logged on by other computers in the organisation is obtained.
  - Prerequisites - Windows Security Auditing.
  - History retention of previously events - 1 year.
  - **On/Off** - *SmartObjects_WindowsSuccessServiceActivityServiceComputer*

- **Scenario 13 - *Windows Failed Service Activity Service***
  - Purpose - to identify, in Microsoft Windows environment, failed authentications for new network services.
  - Description - EventID: 9150061, a new event is generated containing details of the machine in the network on which authentication failed and the new service registered (MS Windows EventID 4625, logon type 5).
  - Prerequisites - Windows Security Auditing.
  - History retention of previously events - 1 year.
  - **On/Off** - *SmartObjects_WindowsFailedServiceActivityService*

- **Scenario 14 - *Windows Failed Service Activity Service User***
  - Purpose - to identify, in Microsoft Windows environment, new failed network logins versus those in the history, of the service type run under a user.
  - Description - EventID: 9150062, a new event is generated containing details of the machine in the network that has logged in, the newly registered service/user combination (MS Windows EventID 4625, logon type 5).
  - Prerequisites - Windows Security Auditing.
  - History retention of previously events - 1 year.
  - **On/Off** - *SmartObjects_WindowsFailedServiceActivityServiceUser*

- **Scenario 15 - *Windows Failed Service Activity Service Computer***
  - Purpose - to identify, in Microsoft Windows environment, new failed network logins versus those in the history, of the service type run on a machine.
  - Description - EventID: 9150063, a new event is generated containing details of the network machine that was logged on, the new service/user combination registered (MS Windows EventID 4625, logon type 5).
  - Prerequisites - Windows Security Auditing.
  - History retention of previously events - 1 year.
  - **On/Off** - *SmartObjects_WindowsFailedServiceActivityServiceComputer*
- **Scenario 16 - *Linux Success Logon Activity SSH***
  - Purpose - to identify, in Linux environments, new SSH logins versus historical ones.
  - Description - EventID: 9150101, a new event is generated containing details of the user and the Linux machine on which SSH was logged in.
  - Prerequisites - Event forwarding.
  - History retention of previously events - 30 days.
  - **On/Off** - *SmartObjects_LinuxSuccessSshdLogonActivity*
- **Scenario 17 - *Linux Success Logon Activity Sudo***
  - Purpose - to identify, in Linux environments, new SUDO logins versus historical ones.
  - Description - EventID: 9150102, a new event is generated containing details of the user and the Linux machine on which SUDO has logged in.
  - Prerequisites - Event forwarding.
  - History retention of previously events - 30 days.
  - **On/Off** - *SmartObjects_LinuxSuccessSudoLogonActivity*
- **Scenario 18 - *Linux Success Logon Activity Su Computer***
  - Purpose - to identify, in Linux environments, new SU logins versus historical ones, organized by computer.
  - Description - EventID: 9150103, a new event is generated containing details of the user and the Linux machine on which the SU has logged in.
  - Prerequisites - Event forwarding.
  - History retention of previously events - 30 days.
  - **On/Off** - *SmartObjects_LinuxSuccessSuComputerLogonActivity*
- **Scenario 19 - *Linux Success Logon Activity Su SrcIP***
  - Purpose - to identify, in Linux environments, new SU logins against historical ones, organized by source IP.
  - Description - EventID: 9150104, a new event is generated containing details of the user and the IP on which the SU logged in.
  - Prerequisites - Event forwarding.
  - History retention of previously events - 30 days.
  - **On/Off** - *SmartObjects_LinuxSuccessSuSrcIPLogonActivity*
- **Scenario 20 - *Linux Failed Logon Activity SSH***
  - Purpose - to identify, in Linux environments, new failed SSH logins versus historical ones.
  - Description - EventID: 9150151, a new event is generated containing details of the user and Linux machine on which the SSH login failed.
  - Prerequisites - Event forwarding.
  - History retention of previously events - 30 days.
  - **On/Off** - *SmartObjects_LinuxFailedSshdLogonActivity*
- **Scenario 21 - *VPN Success Logon Activity by Country***

- Purpose - monitors whether a new username/geolocation combination has successfully logged into the organization on the VPN against history. We only have for openVPN and FortiGate. Organize by country of login.
- Description - EventID: 9150201, a new event is generated containing details of the user and the country from where the VPN login was performed.
- Prerequisites - FortiGate and Qnap.
- History retention of previously events - 30 days.
- **On/Off** - *SmartObjects_VPNByCountrySuccessLogonActivity*

- **Scenario 22 - *VPN Success Logon Activity by ClientIP***
  - Purpose - monitors whether a new username/geolocation combination has successfully logged into the organization on the VPN against history. We only have for openVPN and FortiGate. Organize by IP from where logged in.
  - Description - EventID: 9150202, a new event is generated containing details of the user and the IP from where the VPN login was performed.
  - Prerequisites - FortiGate and Qnap.
  - History retention of previously events - 30 days.
  - **On/Off** - *SmartObjects_VPNByClientIPSuccessLogonActivity*
- **Scenario 23 - *An object was moved from _SourceFile_ to _Destination_***
  - Purpose - to identify, in Microsoft Windows environments, the moved files with the location before and after the move.
  - Description - EventID: 580466301, a new event is generated containing details of the file name and path before and after the move.
  - Prerequisites - Windows Object Access enabled and folder with auditing enabled (at Windows level).
- **Scenario 24 - *An object was deleted***
  - Purpose - to identify, in Microsoft Windows environments, deleted files/objects with the location and name of the file/object.
  - Description - EventID: 580466302, a new event is generated containing details of the name and path of the deleted file.
  - Prerequisites - Windows Object Access enabled and folder with auditing enabled (at Windows level).
- **Scenario 25 - *A file was created or modified***
  - Purpose - to identify, in Microsoft Windows environments, newly created or modified files with the location and file name.
  - Description - EventID: 580466303, a new event is generated containing details about the name and path of the created/modified file.
  - Prerequisites - Windows Object Access enabled and folder with auditing enabled (at Windows level).
- **Scenario 26 - *A new folder was created***
  - Purpose - to identify, in Microsoft Windows environments, newly created folders with location and folder name.
  - Description - EventID: 580466304, a new event is generated containing details about the name and path of the created folder.
  - Prerequisites - Windows Object Access enabled and folder with auditing enabled (at Windows level).
- **Scenario 27 - *An object was renamed from _SourceFile_ to _DestinationFile_***
  - Purpose - to identify, in Microsoft Windows environments, renamed objects with the location and name of the object before and after renaming.
  - Description - EventID: 580466305, a new event is generated containing details of the object name and path before and after renaming.
  - Prerequisites - Windows Object Access enabled and folder with auditing enabled (at Windows level).
- **Scenario 28 - *An object was accessed***

- Purpose - to identify, in Microsoft Windows environments, the accessed objects by mentioning the location and the name of the object.
- Description - EventID: 580466306, a new event is generated containing details of the name and path of the accessed object.
- Prerequisites - Windows Object Access enabled and folder with auditing enabled (at Windows level).

- **Scenario 29 - *Windows Failed Batch Logon Activity***
  - Purpose - to identify, in the Microsoft Windows environment, a failed batch logon against those in history (*for example, a scheduled task*).
  - Description - EventID: 9150013, a new event is generated containing details of the user and the network IP on which he login failed. It also contains historical information about previous batch logins (MS Windows EventID 4625, logon type 4).
  - Prerequisites - Windows Security Auditing.
  - History retention of previously events - 30 days.
  - **On/Off** - *SmartObjects_WindowsFailedBatchLogonActivity*
- **Scenario 30 - *Windows Failed Service Logon Activity***
  - Purpose - to identify, in Microsoft Windows environment, a failed service logon compared to the historical ones (*e.g. Service startup*).
  - Description - EventID: 9150014, a new event is generated containing details of the service and the IP in the network that was login failed. It also contains historical information about previous logins (MS Windows EventID 4625, logon type 5).
  - Prerequisites - Windows Security Auditing.
  - History retention of previously events - 1 year.
  - **On/Off** - *SmartObjects_WindowsFailedServiceLogonActivity*
- **Scenario 31 - *Windows Failed Network Cleartext Logon Activity***
  - Purpose - to identify, in Microsoft Windows environment, a new failed Cleartext authentication type compared to the historical one (where the password is transmitted in clear. Logon with credentials sent in the clear text. Most often indicates a logon to IIS with “basic authentication”).
  - Description - EventID: 9150015, a new event is generated containing details of the user and the IP in the network to which he login failed. It also contains historical information about previous logins (MS Windows EventID 4625, logon type 8).
  - Prerequisites - Windows Security Auditing.
  - History retention of previously events - 30 days.
  - **On/Off** - *SmartObjects_WindowsFailedNetworkCleartextLogonActivity*
- **Scenario 32 - *Windows Failed Remote Interactive Logon Activity***
  - Purpose - to identify, in Microsoft Windows environment, a new failed remote interactive login in addition to the ones in the history (*Terminal Services, Remote Desktop or Remote Assistance*).
  - Description - EventID: 9150016, a new event is generated containing details of the user and network IP that login failed. It also contains historical information about previous logins (MS Windows EventID 4625, logon type 10).
  - Prerequisites - Windows Security Auditing.
  - History retention of previously events - 30 days.
  - **On/Off** - *SmartObjects_WindowsFailedRemoteInteractiveLogonActivity*
- **Scenario 33 - *Windows Failed Cached Interactive Logon Activity***
  - Purpose - to identify, in Microsoft Windows environment, a failed cached login after a break period of at least 3 months.
  - Description - EventID: 9150017, a new event is generated containing details of the user and network IP that login failed. It also contains historical information about previous logins (MS Windows EventID 4625, logon type 11).
  - Prerequisites - Windows Security Auditing.
  - History retention of previously events - 30 days.
  - **On/Off** - *SmartObjects_WindowsFailedRemoteInteractiveLogonActivity*

Automation

Introduction

CYBERQUEST Automation

The **Automation module** in CYBERQUEST enables automated execution of mitigation steps and predefined actions in response to specific events or alerts.

Actions are grouped into **playbooks**, which define structured sequences of operations designed to carry out specific mitigation processes.

Playbooks can be **created, edited, or deleted** through the graphical interface.

Actions and Input Parameters

Each action within a playbook requires specific **input data (parameters)** to function correctly. During playbook configuration, all necessary parameters for each action can be customized.

- Parameters are **dynamic** and their values are automatically determined at runtime when the playbook executes.
- During **playbook debugging** (see the *Troubleshooting* section), the **Execution History** provides detailed information on the input values used for each action execution.

Triggering Playbook execution

Playbooks can be executed in several ways:

- Automatically from alerts
- Manually from Event Browser
- Manually from Alert Browser
- Manually from Case Management

Automatic execution from alerts

A playbook can be automatically triggered by a specific alert.

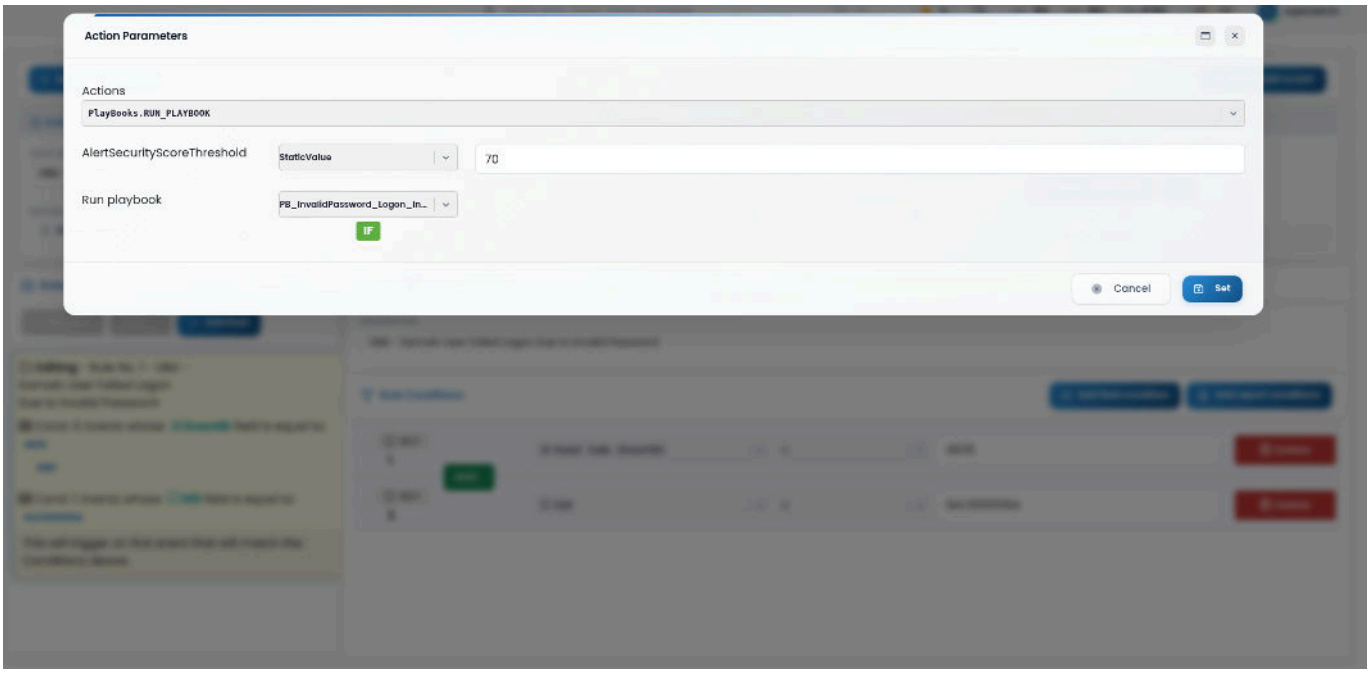
- When an alert is generated, the corresponding playbook is executed automatically.
- The alert instance becomes the **global input data** for the playbook and can be referenced within actions through **placeholders**.

To configure automatic playbook execution for a specific alert:

1.Navigate to **Settings > Alerts > Realtime**

2.Open the alert definition and locate **Has Action**

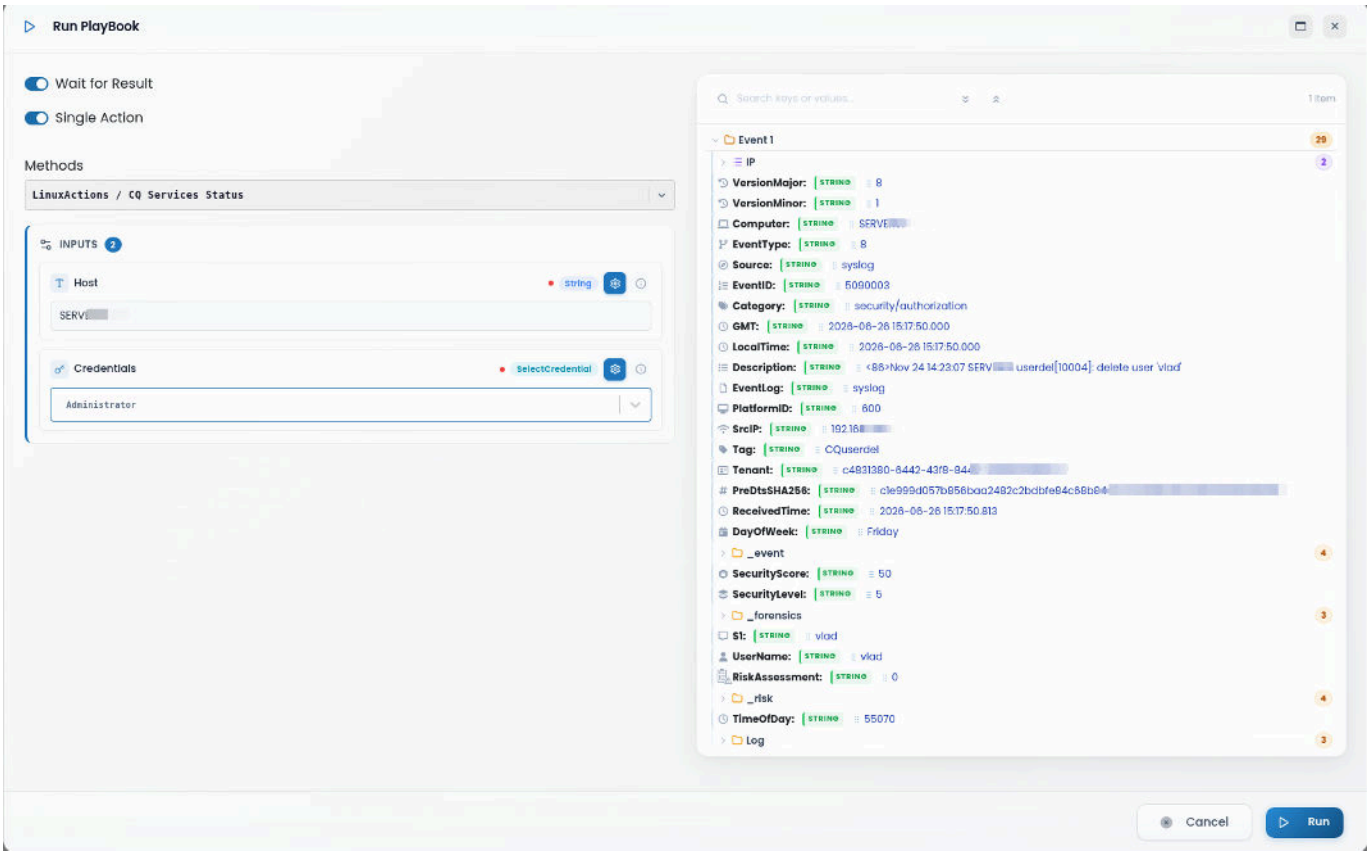
3.Select the **PlayBooks.PLAYBOOK** parameter and choose the playbook to associate with the alert



When the system detects repeated invalid password attempts, an automated playbook is immediately triggered. It opens a predefined investigation case, adds relevant evidence, and notifies the SOC team so they can quickly review and respond.

Manual execution from Event Browser

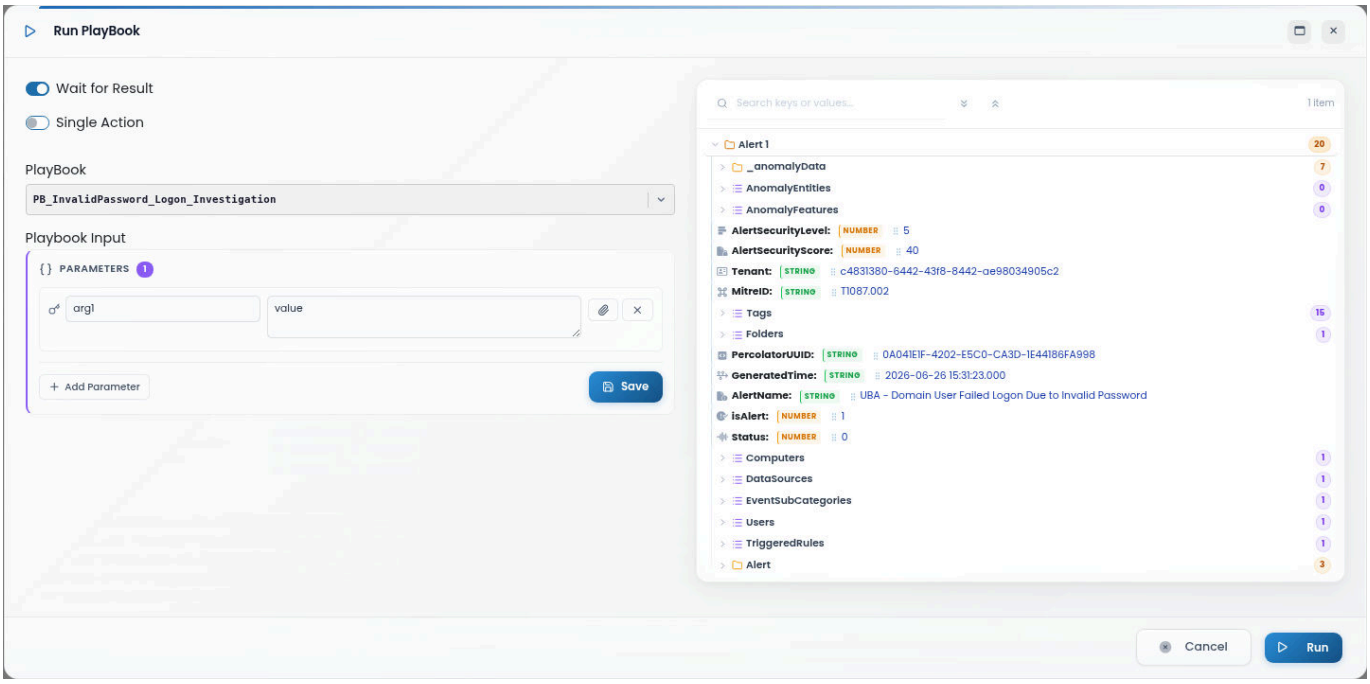
Initiate a playbook manually by selecting a specific event through the interactive GUI.



The playbook runs for that specific event, allowing targeted mitigation without waiting for automatic triggers.

Manual execution from Alert Browser

Initiate a playbook manually by selecting a specific alert through the interactive GUI.



The mitigation flow is applied to the selected alert, providing flexibility to respond to critical alerts on demand.

Refer to **Settings > Management > Playbooks** for instructions on adding or editing mitigation flows.

Action types include:

- **Vendor-specific actions**, such as firewall, EDR, or ticketing system integrations
- **Functional actions**, such as array count, conditional logic (IF), array sum, or custom actions using DTS objects and JavaScript

Specific technologies / vendors

CYBERQUEST includes an **extensive and continually growing list of technology vendors** to support automation of day-to-day mitigation tasks and security administration.

- The vendor list is **automatically updated** with each new release, adding more vendors and actions to the mitigation workflows.
- Many vendors provide **API integrations** with their products. Full API documentation is available on the respective vendor websites.
- A complete list of **supported vendors and available actions** can be found in the **Supported Vendors** section.

This integration allows CYBERQUEST to seamlessly interact with a wide range of third-party systems, enabling **efficient and consistent automated responses** across multiple technologies.

Functional actions

To enable flexible and customized mitigation workflows, CYBERQUEST provides several **functional actions** under the **"CYBERQUEST Playbook"** vendor. These actions help orchestrate responses based on conditions, data, or predefined logic:

- **IF** - Evaluates a specified condition and returns a boolean result. This action allows the workflow to branch into **true/false paths** depending on the evaluation.
- **Count** - Counts the number of elements in a given variable. The variable must be an array; otherwise, execution is interrupted.
- **Code** - Executes a predefined **DTS object**, enabling custom logic or operations within the playbook. DTS object configuration is described in the DTS documentation.

These functional actions make it possible to **create dynamic, conditional, and programmable mitigation flows** tailored to specific scenarios.

Extending Actions

Action definitions

CYBERQUEST automation supports **custom scripted actions** using **JavaScript**, allowing advanced customization of mitigation workflows.

Creating a Custom Action:

1.Add a new **DTS object** in the system.

2.Access incoming data within the script via the **Event object**, which provides all relevant information from the triggering alert or event.

This approach enables the creation of **tailored actions** that can extend standard automation capabilities and handle complex or unique scenarios.

```
// new action to be executed in CQ Automation
// input data can be accessed by employing the "Event"

let currentInputData = Event;

if (currentInputData.EventID==4624 ) // validates a field in the event section
{
    // do something
}
else
{
    // do something else
}
```

JavaScript Customization in DTS

By default, the **JavaScript section** of each DTS object allows full customization of the actions to be performed within a playbook.

- All standard **JavaScript functionality** is supported.
- External data sources, including **APIs**, can be leveraged to implement **custom use cases** and extend automation capabilities.

```
let result = CQ.Communications.HttpRequest.get('https://www.exampleAPI.com');
// result will be an object of HttpResponse

let resultAsJSON = result.asJson();

if (resultAsJSON.exampleResponseProperty=="200"){
    // do something
}
else
{
    //do something else
}
```

All functionality available in the **CYBERQUEST API** is accessible and can be utilized within these objects. For more details, refer to the CYBERQUEST API

Supported Vendors

Supported Vendors/Actions

Technology/Vendor	Action Name	Description	References
AbuseIPDB	PostBulkReport	Reports multple IPs at once	AbuseIPDB (https://docs.abuseipdb.com/#introduction)
	GetCheck	Executes an AbuseIPDB IP lookup using the IP address you provided.	
	GetReports	Get reports about IP address	
	GetBlacklist	Depending on the input settings you have chosen, AbuseIPDB will return a list of all reported IP addresses or a list of a specific subset of reported IP addresses.	
	PostReport	Based on the IP address and malware category you have chosen, reports a specific IP address that has been linked to malicious online activity to AbuseIPDB.	
	GetCheckBlock	Check if the IP is block	
	DeleteClearAddress	Clear IP address	
AlienVault	PostIndicatorsSubmitFile	Analyze suspicious files to quickly detect malware and malicious activity.	AlienVault (https://otx.alienvault.com/assets/static/external_api.html)
	GetUser	Validate your API Key configuration.	
	GetUserWithUsernameAndAction	Perform actions like follow/subscribe to other users by username.	
	GetUsers	Validate your API Key configuration.	
	GetUsersWithUsernameAndAction	Perform actions like follow/subscribe to	

Technology/Vendor	Action Name	Description	References
		other users by username.	
	GetSearchUsers	Search for users matcing query	
	GetSearchPulses	Search for pulses matcing query	
	GetPulsesWithID	View or edit of pulse with id pulse_id. When editing a pulse, use PATCH.	
	PatchPulsesWithID	View or edit of pulse with id pulse_id. When editing a pulse, use PATCH.	
	GetPulsesIndicatorsWithID	Returns paginated list view of the indicators inside the pulse pulse_id.	
	GetPulsesRelatedWithID	Return all pulses that share an indicator with this pulse	
	GetPulsesRelated	Find pulses related to either an existing pulse, a malware family or an adversary.	
	GetPulsesSubscribed	Threat intelligence subscriptions	
	GetPulsesSubscribedPulseIDS	List the ids of all pulses you are subscribed to.	
	GetPulsesActivity	Activity feed consists of pulses: - All pulse subscriptions (directly subscribed to pulse, and all pulses by subscribed to users) - All pulses created by myself - All pulses by users I am following	
	GetPulsesSubscribeWithID	Subscribe to pulse.	
	GetPulsesUnsubscribeWithID	Unsubscribe from pulse.	
	GetPulsesIndicatorsTypes	Returns string representations of each indicator type (i.e. “domain”), as recognized by OTX.	
	GetIndicatorswithDomainandSection	Indicator page api for domain names	
	GetPulsesEvents	List events, such as subscribe/unsubscribe	

Technology/Vendor	Action Name	Description	References
		to user/pulse.	
	GetPulsesUsersWithUsername	Returns authenticated users or passed in user created pulse feed, default sorted by latest modified.	
	GetPulsesMy	Returns your feed of pulses you've created, default sorted by latest modified.	
	GetIndicatorsCorrelationRuleWithCorrelationRuleAndSection	Indicator page api for Correlation Rules	
	PostIndicatorsUpdateSubmittedURLsTLP	Update the TLP level of previously submitted URLs.	
	PostIndicatorsSubmitURL	This is an endpoint to submit a single url at once.	
	GetIndicatorsNidsWithNidsAndSection	Indicator page api for NIDSs	
	GetIndicatorsCVEWithCVEAndSection	Indicator page api for CVEs (MITRE's Common Vulnerability Enumeration)	
	GetIndicatorsURLWithURLWithSection	Indicator page api for URLs	
	GetIndicatorsFileWithFilehashAndSection	Indicator page api for files (file hashes)	
	GetIndicatorsHostnameWithHostnameAndSection	Indicator page api for hostname names	
	GetIndicatorsIPv6WithIPAndSection	Indicator page api for IPv6 Addresses	
	GetIndicatorsIPv4WithIPAndSection	Indicator page api for IPv4 Addresses	
	GetIndicatorsSubmittedURLs	Returns a list of all submitted URLs, along with the status of the submission.	
	GetIndicatorsSubmittedFiles	Returns a list of all submitted files, along with the status of the submission.	
ApiVoid	GetThreatLog	This API lets you query ThreatLog.com database of malicious domains.	ApiVoid (https://docs.apivoid.com/)
	GetIPReputation	This API lets you check the reputation and geolocation of an IPv4 address.	

Technology/Vendor	Action Name	Description	References
	GetDomainReputation	This API lets you check if a domain name is blacklisted by trusted sources.	
	GetScreenshot	This API lets you take high-quality screenshots of any web page and URL.	
	GetURLReputation	This API can help you identify potentially unsafe and phishing URLs.	
	GetDomainAge	This API lets you get domain registration date and domain age in days.	
	GetSiteTrustworthiness	This API provides you important details about a website to check if it is legit.	
	GetParkedDomain	This API lets you check if a domain name is parked/for sale.	
	GetURLStatus	This API lets you check if an URL is online or offline (down or not accessible).	
	GetDNSPropagation	This API lets you check if DNS records of a domain have propagated globally.	
	GetURLtoHTML	This API lets you capture the HTML page source after JavaScript has been executed.	
	GetSSLInfo	This API provides you details about a website's SSL certificate.	
	GetEmailVerify	This API provides you useful information about an email address.	
	GetReverseIP	This API lets you find a list of domains hosted on the same IPv4 address.	
	GetSPFValidator	This API lets you check and validate SPF record of any domain.	
	GetHTTPTracker	This API lets you check HTTP requests made	

Technology/Vendor	Action Name	Description	References
		by an URL or a website.	
	GetURLtoPDF	This API lets you convert an URL into a high-quality PDF document.	
	GetDNSLookup	This API lets you easily get DNS records of domain names.	
Blocklist.de	GetAllIPAddressesByType	All IP addresses that have attacked one of our customers/servers in the last 48 hours.	Blocklist.de (https://www.blocklist.de/en/api.html)
	GetLastAddedIPAddresses	Get only the last added IP Adresses	
	GetLastAddedIPAddressesApi	The API can currently only issue attacks and reports per user, server or ip-address.	
BOTVRIJ.EU	GetBOTVRIJEU	Botvrij.eu provides different sets of open source IOCs that you can use in your security devices to detect possible malicious activity.	BOTVRIJ.EU (https://www.botvrij.eu/https://www.botvrij.eu/)
CheckPhish	PostSubmitURL	Submit URL for Scan	CheckPhish (https://checkphish.ai/docs/checkphish-api/)
	PostGetResultsByQuery	GetSearchByTerm	
Cymon	PostLogin	Authenticate with username and password to get a JSON Web Token.	Cymon (https://cymon.docs.apiary.io/#reference/feeds/update-feed/update?console=1)
	GetSearchByIP	Search threat reports by IP address (IPv4 and IPv6).	
	GetSearchByDomain	Search threat reports by domain name.	
	GetSearchByHostName	Search threat reports by hostname.	
	GetSearchByMD5	Search threat reports by MD5 hash.	
	GetSearchBySHA1	Search threat reports by SHA1 hash.	

Technology/Vendor	Action Name	Description	References
	GetSearchBySHA256	Search threat reports by SHA256 hash.	
	GetSearchBySSDEEP*	Search threat reports by SSDEEP hash.	
	GetSearchByTerm	Search threat reports by a term.	
	GetSearchByFeedID	Get threat reports in a feed.	
	GetListAllFeeds	Get paginated list of feeds.	
	GetFeedDetails	Get feed object.	
	GetUserFeeds	Get paginated list of feeds that user has access to.	
	GetReportDocument	Get threat report from feed.	
	PostCreateFeed	Create a new feed for threat reports.	
	PutUpdateFeed	Update details of an existing feed.	
	PostSubmitReport	Upload a threat report with observables.	
	PostSubmitReportBulk	Upload multiple threat reports in one request.	
Dshield	GetIP	Returns a summary of the information our database holds for a particular IP address	Dshield (https://www.dshield.org/api/)
	GetThreatfeeds	The DShield server is the source of retrieval for open threat feeds.	
Feodo Tracker	GetBotnetC2IPBlocklist	Get IP Blocklist	FeodoTracker (https://feodotracker.abuse.ch/blocklist/)
	GetBotnetC2IPBlocklistCustomFormat	Get IP Blocklist	
	GetBotnetC2IndicatorsOfCompromiseSIEM	Get Indicators of Compromise	
	GetBotnetC2IndicatorsOfCompromiseAggressive	Get Indicators of Compromise	
FortiOS	GetUserFirewall	Display a list of authenticated users on the firewall.	
	GetUserBanned	Retrieve a list of all users who have been	

Technology/Vendor	Action Name	Description	References
		banned based on their IP addresses.	
	GetCollectedEmail	Retrieve a list of email addresses that have been collected from the captive portal.	
	GetFortiguardServiceCommunicationStats	Retrieve historical statistics for use with FortiGuard services.	
	GetFortiviewStatistics	Get drill-down and summary data for FortiView (both in real time and in the past).	
	GetWebfilterMaliciousUrls	Obtain a list of all URLs in the FortiSandbox harmful URL database.	
	GetMaliciousUrlsStat	Get FortiSandbox malicious URL database statistics.	
	GetRouterIPv4	List all IPv4 routing table entries that are currently active.	
	GetRouterIPv6	List all IPv6 routing table entries that are currently active.	
	GetRouterStatistics	Retrieve routing table statistics, including the number of matched routes.	
FortiOSConfigurationFirewall	SetFirewallPolicyBlockAddress	Is able to configure a FortiOS (FOS) device by allowing the user to set a firewall policy to block the specified address.	
HoneyDB	GetBadHosts	Retrieve a list of bad hosts from HoneyDB	HoneyDB (https://documenter.getpostman.com/view/2358963/SVtTzopj?version=latest#3fb7c51f-10de-406e-9797-13f51c8a9902)
	GetBadHostsFiltered	Returns the data provided by the user to HoneyDB	
	GetBadHostsService	Retrieve a list bad hosts by service name.	
	GetBadHostsServiceFiltered	Retreive bad hosts by service name	

Technology/Vendor	Action Name	Description	References
		provided by the user to HoneyDB	
	GetIPHistoryHost	IP (bad host) history is a summary of all interaction activity for a certain IP address recorded by the HoneyDB network.	
	GeSensorDataCount	If you have sensors that log data to HoneyDB, you can use this API to get a count of sensor event data collected for a specified date.	
	GetSensorData	If you have sensors that log data to HoneyDB, you may use this endpoint to get all sensor event data collected for a specified date.	
	GetSensorDataFiltered	If you have sensors that log data to HoneyDB, you may use this endpoint to get all sensor event data collected for a specified date.	
	GetServices	Return a list of services that are used	
	GetIPInfoTor	Returns true or false to indicate if the IP provided is a Tor exit node.	
	GetStats	Services are the network protocols emulated by honeypot sensors.	
	GetStatsAsn	Return a list of asn	
	GetTwitterThreatFeed	The Twitter threat feed includes a list of problematic hosts that have connected or attempted to connect to other honeypots on the Internet (including honeypots that do not submit data directly to HoneyDB).	
	GetTwitterThreatFeedHost	Twitter threat feed data filtered by host (IP address).	

Technology/Vendor	Action Name	Description	References
	GeNodes	Honeydb-agent sensors are deployed on nodes. This endpoint delivers all nodes viewed within the last three days.	
	GetNodesFiltered	Honeydb-agent sensors are deployed on nodes. This endpoint delivers all nodes viewed within the last three days. Informations provided by the user	
	GetPayloadHistoryYear	IP (bad host) history (year) is a list of all interactions recorded by the HoneyDB network for a specific IP address.	
	GetPayloadHistoryYearMonth	IP (bad host) history (month with year) is a list of all interactions recorded by the HoneyDB network for a specific IP address.	
	GetPayloadHistoryService	IP (bad host) history (service) is a list of all interactions recorded by the HoneyDB network for a specific IP address.	
	GetPayloadHistoryHash	IP (bad host) history (hash) is a list of all interactions recorded by the HoneyDB network for a specific IP address.	
	GetInternetScanner	Returns true or false depending on if the provided IP address is part of a known Internet scanning service.	
	GetInternetScannerInfo	Returns true or false based on whether the supplied IP address is part of a known Internet scanning service, as well as other scanning-related information.	
	GetIPInfo	Returns true or false to show whether the provided IP address is on a known IP list.	

Technology/Vendor	Action Name	Description	References
	GetIPInfoBogon	Returns true or false to indicate if the IP provided is bogon IP address.	
	GetIPInfosSansip	Returns true or false to indicate if the IP provided is on the SANS IP list	
	GetIPInfoCiarmy	Returns true or false to indicate if the IP provided is on the The CINS Army List.	
	GetIPInfoEtCompromised	Returns true or false to indicate if the IP provided is on the Emerging Threats Compromised IP list.	
	GetIPInfoProjectHoneypot	Returns true or false to indicate if the IP provided is on the Project Honeypot list and additional threat data.	
	GetNetInfoLookup	Returns AS, network information and geolocation for an IP address.	
	GetNetInfoNetworkAddresses	Returns all IP addresses as part of a network range.	
	GetNetInfoPrefixes	Returns all prefixes advertised for a specific AS network.	
	GetNetInfoAsName	Returns the name of the AS network.	
	GetNetInfoGeolocation	Geolocation information for an IP address is returned.	
	GetDatacenterAWS	Returns AWS IP ranges.	
	GetDatacenterAzure	Returns Azure IP ranges.	
	GetDatacenterAzureChina	Returns Azure China IP ranges.	
	GetDatacenterAzureGermany	Returns Azure Germany IP ranges.	
	GetDatacenterAzureGov	Returns Azure Gov IP ranges.	
	GetDatacenterGcp	Returns Google Cloud IP ranges.	
	GetDatacenterOracle	Returns Oracle Cloud IP	

Technology/Vendor	Action Name	Description	References
		ranges.	
Host.io	GetWebDomain	Metadata scraped from a domain homepage.	Host.io (https://host.io/docs)
	GetDNSDomain	Get all the DNS records stored for a domain.	
	GetRelatedDomain	Get a count of the number of related domains for all supported lookups offered by Host.io	
	GetFullDomain	A single endpoint that includes the data from all APIs from above	
	GetDomainsFieldValue	Get all domains associated with a field	
IP-API	GetIPGeolocation	Return Geolocation informations	IP-API (https://ip-api.com/docs)
	Batch IP Geolocation	Batch processing gives you the ability to query multiple IP addresses in one HTTP request	
IPinfo.io	Geolocation Data	It includes country, region, city, and postal code of the target IP	IPinfo.io (https://ipinfo.io/developers/hosted-domains)
	GetSearchNetRecordsByIPOrIPRange	Return records by IP or IP range	
IPStack	GetStandardIPLookup	Look up for single IPv4 or IPv6 addresses	IPStack (https://ipstack.com/documentation)
	GetRequesterIPLookup	Look up for the ip from which the request comes	
Kuudos	GetListOfApplications	List of applications (apks)	Kuudos (https://docs.kodous.com/api/apks.html)
	GetDetailedInformationAboutAnAPK	An apk's detailed information.	
	GetUploadUrl	Create a link for an apk upload.	
	GetStaticAndDynamicAnalysisReport	Get a copy of the static and dynamic analysis reports.	

Technology/Vendor	Action Name	Description	References
MacVendors	GetLookupMacAddress	This API performs a quick and easy vendor lookup for mac addresses.	MacVendors (https://macvendors.com/app/home)
Mailboxlayer	GetEmailCheck	Validates and verifies an email address in order to determine deliverability and quality.	Mailboxlayer (https://apilayer.com/marketplace/email_verification-api?live_demo=show)
	GetEmail	Validates and verifies an email address in order to determine deliverability and quality.	
Malshare	GetListHashesJSON	List hashes from the past 24 hours	Malshare (https://malshare.com/doc.php)
	GetListHashesForASpecificFormat	List MD5/SHA1/SHA256 hashes of a specific type from the past 24 hours	
	GetListSamplesRaw	List of sample sources from the past 24 hours	
	GetTypes	Get list of file types & count from the past 24 hours	
	GetListHashesRaw	List hashes from the past 24 hours	
	GetDownloadFile	Download File	
	GetStoredFileDetails	GET stored file details	
	GetListSamplesJSON	List of sample sources from the past 24 hours	
	GetSearch	Search sample hashes, sources and file names	
	GetListOfFileNames	Returns a list of file names from recent uploads.	
OCR	PostConvertImageFromURL	Convert a image from an URL	OCR (https://ocr.space/OCRAPI)
	PostConvertPDFFromURL	Convert a PDF from a URL	

Technology/Vendor	Action Name	Description	References
	PostConvertImageFromBASE64String	Convert a image from an BASE64 String	
	PostCreateSearchablePDFFromImage	Create Searchable PDF from image	
OpenAI	PostCreateChatCompletion	Interaction with ChatGPT API	OpenAI (https://platform.openai.com/docs/api-reference/introduction)
RIPEstat	GetAbuseContactFinder	This data call's primary goal is to return abuse contact information for an Internet number resource.	RIPEstat (https://stat.ripe.net/docs/02.data-api/)
	GetAddressSpaceHierarchy	This data call returns address space objects (inetnum or inet6num) from the RIPE Database related to the queried resource.	
	GetAddressSpaceUsage	This data call displays the usage of a prefix or IP range based on the objects currently in the RIPE database.	
	GetAllocationHistory	This data call returns information supplied by IANA and RIRs for allocations and direct assignments of prefixes and AS numbers of time.	
	GetAnnouncedPrefixes	This API request provides a list of announced IP prefixes associated with a given ASN. The results can be filtered based on a specific time frame if desired.	
	GetAsOverview	This data call provides an overview of an ASN, including its announcement status and the name of its holder based on the WHOIS service.	
	GetASPatchLength	This data call retrieves AS-path metrics for the queried ASN, such as the shortest or longest AS-path to other ASNs	

Technology/Vendor	Action Name	Description	References
		that we are peering with.	
	GetASRoutingConsistency	This data call examines the consistency between the registration information for an ASN in the internet routing registry (IRR) and what is observed in RIS' BGP tables.	
	GetASNNeighbours	This data call provides information on the network neighbors for a given ASN as observed in RIS. It includes statistical information and the list of observed ASN neighbors.	
	GetASNNeighboursHistory	This data call provides information about the neighboring ASNs of a queried ASN, extended with historical data. It includes details about the ASNs that have been observed as neighbors over time.	
	GetAtlasProbeDeployment	This data call provides information on the number of RIPE Atlas probes in a region, a country or network (ASN).	
	GetAtlasProbes	This data call returns information on RIPE Atlas probes in an ASN, a prefix, or a country.	
	GetAtlasTargets	This data call provides information on the RIPE Atlas measurements that target an network (ASN), a prefix or a hostname.	
	GetBGPState	This data call delivers the state of BGP routes for a resource as observed by all RIS collectors at a given point in time.	
	GetBGPUpdateActivity	The number of BGP updates seen over time is returned by this data request. The	

Technology/Vendor	Action Name	Description	References
		aggregated results are shown in time intervals whose length is determined by the input parameters.	
	GetBGPUpdates	This data call returns the BGP updates for a resource over a specified time period.	
	GetBGPlay	This data call represents the scenario of what occurred to the BGP routes of a resource over a period of time.	
	GetBlocklist	This data call returns blocklist related data for a queried resource.	
	GetCountryASN	This data call returns information on the registered and routed ASNs of a country.	
	GetCountryResourceList	This data call returns information about the Internet resources associated with a country, such as ASNs, IPv4 ranges, and IPv4/6 CIDR prefixes.	
	GetCountryResourceStats	This data call returns information about a country's Internet resources.	
	GetDNSChain	This data call returns the recursive chain of DNS forward (A/AAAA/CNAME) and reverse (PTR) records starting form either a hostname or an IP address.	
	GetWhoisObjectLastUpdated	This data call returns information of when a certain object was last updated in the whois database.	
	GetWhois	This data call returns whois information from the relevant Regional Internet Registry and Routing Registry.	
	GetWhatsMyIp	This data call returns the IP address of the requester	

Technology/Vendor	Action Name	Description	References
	GetVisibility	This data call provides information on the visibility of a resource as observed from RIS	
	GetSpeedcheckerBandwidthMeasurements	This data call provides bandwidth measurement results collected on the Speedchecker platform.	
	GetSearchComplete	This data call returns example resource that are directly or indirectly related to the given input.	
	GetRRCInfo	This data call provides (meta) information on collector nodes (RRCs) of the RIS network	
	GetRPKIValidationStatus	This data call returns the RPKI validity state for a combination of prefix and Autonomous System. This combination will be used to perform the lookup against the RPKI validator Routinator, and then return its RPKI validity state.	
	GetRPKIHistory	This data call returns a timeseries with the count of VRPs (Validated ROA Payload) for the requested resource. The data source of this endpoint are the files hosted in ftp.ripe.net/rpki.	
	GetRoutingStatus	This data call returns a summary of the current BGP routing state of a given IP prefix or ASN, as observed by the RIS route collectors	
	GetRoutingHistory	This data call shows the history of announcements for prefixes, including the origin ASN and the first hop.	
	GetRISPrefixes	This data call provides information on prefixes related to an ASN. The	

Technology/Vendor	Action Name	Description	References
		data call distinguishes prefixes in the originated and transited ASN.	
	GetRISPeers	This data call provides information on the peers of RIS - ASN, IP address and number of shared routes. The data is grouped by RIS collectors.	
	GetRISPeerings	This data call returns routes for advertisements of a given IP resource, or that are originated from a given ASN, as seen by the RIPE NCC route collectors	
	GetPeerCount	This data call provides information on the number of peers as seen by RIS	
	GetRISFullTableTreshhold	This data call provides the cut-off threshold for the number of prefixes that a BGP full-table peer requires to have.	
	GetRISFirstLastSeen	This data call provides information on when a prefix or ASN was first and last seen in RIS data.	
	GetRISAsns	This data call provides high-level information on ASNs in RIS	
	GetRIRStatsCountry	This data call returns geographical information for Internet resources based on RIR Statistics data.	
	GetRIRPrefixSizeDistribution	This data call returns the number of allocations and assignments (below the queried resource) according to registration data provided by Regional Internet Registries.	
	GetRIRGeo	This data call returns geographical information for Internet	

Technology/Vendor	Action Name	Description	References
		resources based on RIR Statistics data.	
	GetRIR	This data call shows which RIR(s) allocated/assigned a resource. Depending on the level of detail (“lod” parameter) this can include additional information like registration status or country of registration. The data is based on RIR stats files	
	GetReverseDNSConsistency	This data call returns details on the reverse DNS delegations and its consistency with routed and registered IP space. The input can be a single prefix or an ASN, in which case all routed and registered prefixes for this ASN are used as an input.	
	GetReverseDNSIP	This is just a simple lookup for the reverse DNS info against a single IP address.	
	GetReverseDNS	This data call returns details of reverse DNS delegations for IP prefixes in the RIPE region.	
	GetPrefixSizeDistribution	This data call returns the total amount of prefixes announced by a given ASN per subnet size and IP version.	
	GetPrefixRoutingConsistency	This data call compares the given routes (prefix originating from an ASN) between Routing Registries and actual routing behaviour as seen by the RIPE NCC route collectors (RIS).	
	GetPrefixOverview	This data call gives a summary of the given prefix, including whether and by whom it is announced.	
	GetPrefixCount	This data call shows the number of prefixes	

Technology/Vendor	Action Name	Description	References
		announced by a given ASN over time.	
	GetNetworkInfo	This data call returns the containing prefix and announcing ASN of a given IP address.	
	GetMLabClients	This data call returns a set of all the hosts within a certain resource for which any network tests occurred.The data is based on active host measurements collected by the Measurement Lab platform (M-Lab).	
	GetMLabBandwith	This data call returns a set of all the measured network bandwidths for a certain resource. The data is based on active host measurements collected by the Measurement Lab platform (M-Lab).	
	GetMLabActivityCount	This data call returns a count of all the hosts within a certain resource for which any network tests occurred. The data is based on active host measurements collected by the Measurement Lab platform (M-Lab).	
	GetMeterBandwithMeasuraments	This data call returns bandwidth measurement results based on open data provided by meter.net.	
	GetMaxmindGeoLiteAnnouncedByAS	This data call returns geolocation information for prefixes that are announced by an autonomous system.	
	GetMaxmindGeoLite	This data call returns geolocation information for the given IP space based on MaxMind's GeoLite2 data source.	

Technology/Vendor	Action Name	Description	References
	GetLookingGlass	This data call returns information coming from a Looking Glass.	
	GetHistoricalWhois	This data call provides information on objects that are stored in the RIPE DB.	
	GetExampleResources	This data call returns ASN, IPv4 and IPv6 sample resources.	
ScreenShotMachine	GetScreenShot	This API provide a service to create screenshot or thumbnail of any online web page	ScreenShot Machine (https://www.screenshotmachine.com/)
Sublime Security	GetEmailRep	EmailRep uses hundreds of data points from social media profiles, professional networking sites, dark web credential leaks, data breaches, phishing kits, phishing emails, spam lists, open mail relays, domain age and reputation, deliverability, and more to predict the risk of an email address.	SublimeSecurity (https://docs.sublimesecurity.com/reference/emailrep-introduction)
Threat Intelligence Platform	GetAListOfDomainsResolvingToAnIP	Retrieve a list of domain names resolving to a given IP address, including subdomains.	ThreatIntelligence (https://threatintelligenceplatform.com/login)
	CheckIfADomainIsConsideredDangerous	For a given domain name, check if it is considered to be dangerous in different security data sources. Dangerous domains could be related to a malware distribution network or host a malicious code.	
	GetADomainReputationScoreV1	Evaluate a domain's reputation based on numerous security data sources as well as on an instant host's audit procedure.	

Technology/Vendor	Action Name	Description	References
	GetADomainReputationScoreV2	Evaluate a domain's reputation based on numerous security data sources as well as on an instant host's audit procedure.	
	GetDomainInfrastructureEntries	Get a list of web, mail, and name servers for a particular domain name. Determine the IP address, geolocation, and subnetwork information for each infrastructure entry.	
	GetADomainSSLCertificateChain	For a given domain name, get detailed information about its SSL Certificate and the complete SSL Certificate chain.	
	CheckSSLConfiguration	For a given domain name, establish and test SSL connection to the host and analyze how it is configured - to detect common configuration issues potentially leading to vulnerabilities.	
ThreatMiner	GetDomain	Based on the query, this function returns threat analysis details for the provided domain.	ThreatMiner (https://www.threatminer.org/api.php)
	GetIP	Based on the query, this function returns threat analysis details for the provided ip.	
	GetSamples	Samples for different query type	
	GetImportHash	Retrieves the data that detect the level of similarity between two files at the binary level.	
	GetSSDeep	The Binary File Similarity API allows you to retrieve data that measures the degree of similarity between two files at the binary level. This feature provides information on the level of similarity between the contents of the files, helping to	

Technology/Vendor	Action Name	Description	References
		identify any resemblances or commonalities between them.	
	GetSSL	Based on the query, this function returns hosts or report tagging	
	GetEmail	The Email (Reverse WHOIS) functionality enables you to perform domain searches based on the name, address, telephone number, email address, or physical address of the Registrant as listed in both current and historical Whois records. This feature provides a convenient way to retrieve domain information by utilizing various search criteria associated with the Registrant's details.	
	GetAVDetection	Based on query, this function return Report tagging or samples	
	GetAPTNotes	Based on query, receive different notes	
	GetSearchAPTNotes	Based on query, receive different reports	
Twilio	PostMakeUnboundCalltoaPhoneNumber	Twilio is used to make an outgoing call from one phone to another.	Twilio (https://www.twilio.com/docs/voice/make-calls)
	PostSendMessage	Twilio is used to send an SMS message from one phone to another.	Twilio (https://www.twilio.com/docs/api?filter-product=SMS)
Unshorten.me	GetUnshorten	Un-shorten URLs created by different services	Unshorten.me (https://unshorten.me/api)
Urlscan.io	PostSubmission	The submission API allows you to submit a URL to be scanned and set some options for the scan.	Urlscan.io (https://urlscan.io/)

Technology/Vendor	Action Name	Description	References
	GetSearch	The result has high-level metadata about the scan result and a link to the API for the full scan result.	
	GetResult	Receive results from url submitted	
VulnDB	PostRequest	Get informations about: vulnerabilities, vendors, products (based on what parameters are provided)	VulnDB (https://vuldb.com/?kb.api)
WhatIsMyBrowser	PostBrowserBotDetection	Detect the requesting software/agent	WhatIsMyBrowser (https://developers.whatismybrowser.com/api/)
	GetUserAgentDatabaseSearch (401)	Search in User Agent Database	
	GetUserDatabaseDumpURL (401)	Download User Agent Database	
Chainabuse	GetReports	This API allows users to screen addresses and URLs to verify whether they have been reported as linked to malicious activity on Chainabuse.	Chainabuse (https://docs.chainabuse.com/reference/reports-l)
	GetSingleReport	This API allows users to retrieve a specific report using its ID.	
CISCO	GetMerarkiNetworkSyslogServers	List the syslog servers for a network	CISCO (https://developer.cisco.com/meraki/api-v1/create-organization-action-batch/)
	GetMerarkiTrafficAnalysis	Return the traffic analysis settings for a network	
	GetMerarkiNetworkTraffic	Return the traffic analysis data for this network. Traffic analysis with hostname visibility must be enabled on the network.	

Technology/Vendor	Action Name	Description	References
	GetMerarkiNetworkHealth	Get the channel utilization over each radio for all APs in a network	
	GetMerarkiNetworkHealthAlerts	Return all global alerts on this network	
	PostCreateOrganizationAdaptivePolicyAcl	Creates new adaptive policy ACL	
	PutUpdateOrganizationAdaptivePolicyAcl	Updates an adaptive policy ACL	
	DeleteOrganizationAdaptivePolicyAcl	Deletes the specified adaptive policy ACL. Note this adaptive policy ACL will also be removed from policies using it	
	PostCreateOrganizationAdaptivePolicyGroup	Creates a new adaptive policy group	
	PutUpdateOrganizationAdaptivePolicyGroup	Updates an adaptive policy group. If updating Infrastructure, only the SGT is allowed. Cannot update Unknown	
	PostCreateOrganizationAdaptivePolicyPolicy	Add an Adaptive Policy	
	PutUpdateOrganizationAdaptivePolicyPolicy	Update an Adaptive Policy	
	DeleteOrganizationAdaptivePolicyPolicy	Delete an Adaptive Policy	
FireEye	PostSubmitURLsAnalysis	This endpoint submits a list of URLs for analysis. The limit is 5 URLs in a single call.	FireEye (https://fireeye.dev/apis/detection-on-demand/)
	GetSingleReportWithReportID	This endpoint fetches the results of a single file submission, known as a report	
	GetSingleReportWithMD5orSHA256	This endpoint fetches the latest results for file submission with the provided md5 or sha256 hash.	
	GetArtifacts	This endpoint fetches artifacts, like a screenshot gif file, for the given report_id	
CheckPoint	PostShowLogs	Showing logs according to the given filter.	CheckPoint (https://sc1.checkpoint.com/document

Technology/Vendor	Action Name	Description	References
			s/latest/APIs/?#web/set-smart-task~v1.9%20)
	PostCreateSmartTask	Create a new Smart Task. This command is available only in a Security Management environment or in Multi-Domain environment when logged into local domain.	
	PostShowSmartTask	Create a new Smart Task. Retrieve existing object using object name or uid. This command is available only in a Security Management environment or in Multi-Domain environment when logged into local domain.	
	PostSetSmartTask	Edit existing object using object name or uid.	
	PostAddDomain	Create a new domain in a Multi-Domain-Management environment	
	PostShowDomain	Create a new domain in a Multi-Domain-Management environment. In order to allow administrators to connect to this domain using SmartConsole, use add-trusted-client command.	
	PostSetDomain	Edit domain object using domain name or UID. When the list of domain servers is edited, the command is handled asynchronously.	
	PostAddAccessRule	Create a new access control rule in CheckPoint.	AddAccessRule (https://sc1.checkpoint.com/documents/latest/APIs/index.html#web/add

Technology/Vendor	Action Name	Description	References
			-access-rule~v1.9.1%20)
	PostDeleteAccessRule	Delete an access control rule in CheckPoint.	DeleteAccessRule (https://sc1.checkpoint.com/documents/latest/APIs/index.html#web/delete-access-rule~v1.9.1%20)

Troubleshooting

Every **playbook execution** in CYBERQUEST is fully logged. The system records all variables and input parameters used in each action, providing a complete view of the execution flow.

By reviewing the values recorded for each step or action, it is possible to **debug and inspect the playbook**, identify issues, and ensure that the mitigation workflow behaves as expected.

How to Use Execution Logs

1.Navigate to the **Execution History** section: Execution History

2.Select the playbook run to review.

3.Inspect each action to see:

- Input parameters
- Output results
- Any errors or warnings

Common Troubleshooting Scenarios

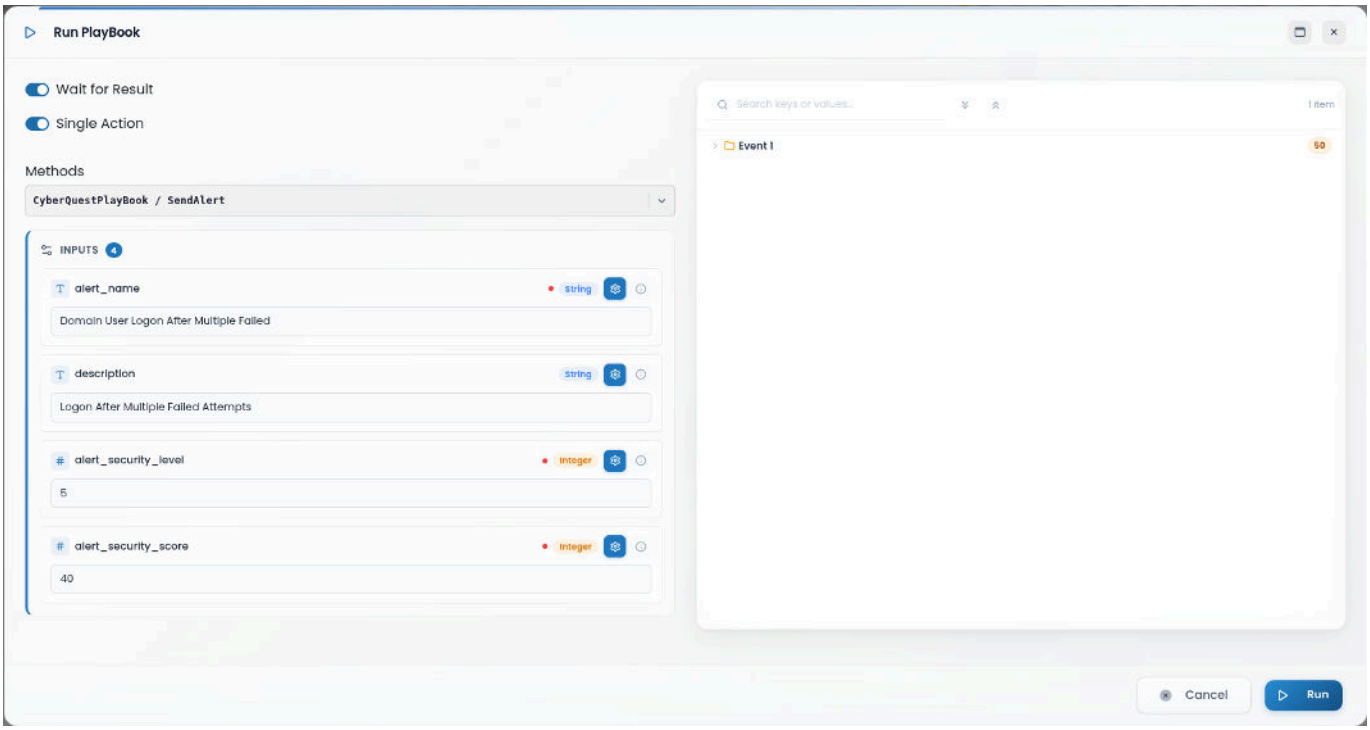
- **Action fails to execute:**
  - Check the input parameters for missing or invalid values.
  - Ensure any required external integrations (APIs, DTS objects) are correctly configured.
- **Unexpected output:**
  - Review the input values for each step in the execution history.
  - Verify logic in conditional actions (e.g., IF statements, custom scripts).
- **Playbook stops mid-execution:**
  - Confirm that array-based actions like **Count** receive valid arrays.
  - Check for script errors in custom DTS objects.
- **External API actions fail:**
  - Verify API credentials and endpoint availability.
  - Ensure network access is allowed from the CYBERQUEST server to the external service.

Automated Actions

Explanation of automated actions

CyberQuestPlayBook/SendAlert method

This action generates an alert with a provided parameters.



Inputs	Description
alert_name (is required)	The name that will be used in the alert
description	The drescription that will be used in the alert
alert_security_level (is required)	The alert security level that will be used in the alert
alert_security_score (is required)	The alert security score that will be used in the alert

CyberQuestPlayBook/IF method

IF node evaluates the condition and directs the flow through the green output if the evaluation is TRUE otherwise through the red output if the evaluation is FALSE.

Inputs	Description
condition (is required)	Condition which will be evaluated

This action is intended to work in a playbook not to be used in a single action.

CyberQuestPlayBook/Code method

Code node is using a DTS object from CYBERQUEST to modify/enrich the playbook data flow with custom functionality which is defined by the user.

Inputs	Description
DTS (is required)	DTS, or Data Transformation Services, is a JavaScript-based parsing service with multifunctional capabilities. Its main function is to perform advanced transformations on data derived from gathered events

CyberQuestPlayBook/Eval method

This action it's used to evaluate a condition and stop the playbook if it failes.

Inputs	Description
condition (is required)	Condition which will be evaluated



This action is intended to work in a playbook not to be used in a single action.

CyberQuestPlayBook/Count method

This operation determines the number of elements present in the array.

Inputs	Description
Left Argument (is required)	The argument which you want to count
Operation (is required)	The operation which is used to count the arguments
Right Argument (is required)	The value of the count



This action is intended to work in a playbook not to be used in a single action.

CyberQuestPlayBook/RunPlayBook method

Enables the execution of a pre-existing playbook.

Inputs	Description
PlayBook (is required)	The name of the playbook which you want to run
Playbook Input (is required)	The input of the playbook



This action is intended to work in a playbook not to be used in a single action.

CyberQuestPlayBook/ForEachRunPlayBook method

Enables the execution of a pre-existing playbook by a number of times.

Inputs	Description
PlayBook (is required)	The name of the playbook which you want to run
Playbook Input (is required)	The input of the playbook
Iterated Variable (is required)	The variable which indicates how many times the playbook will be executed



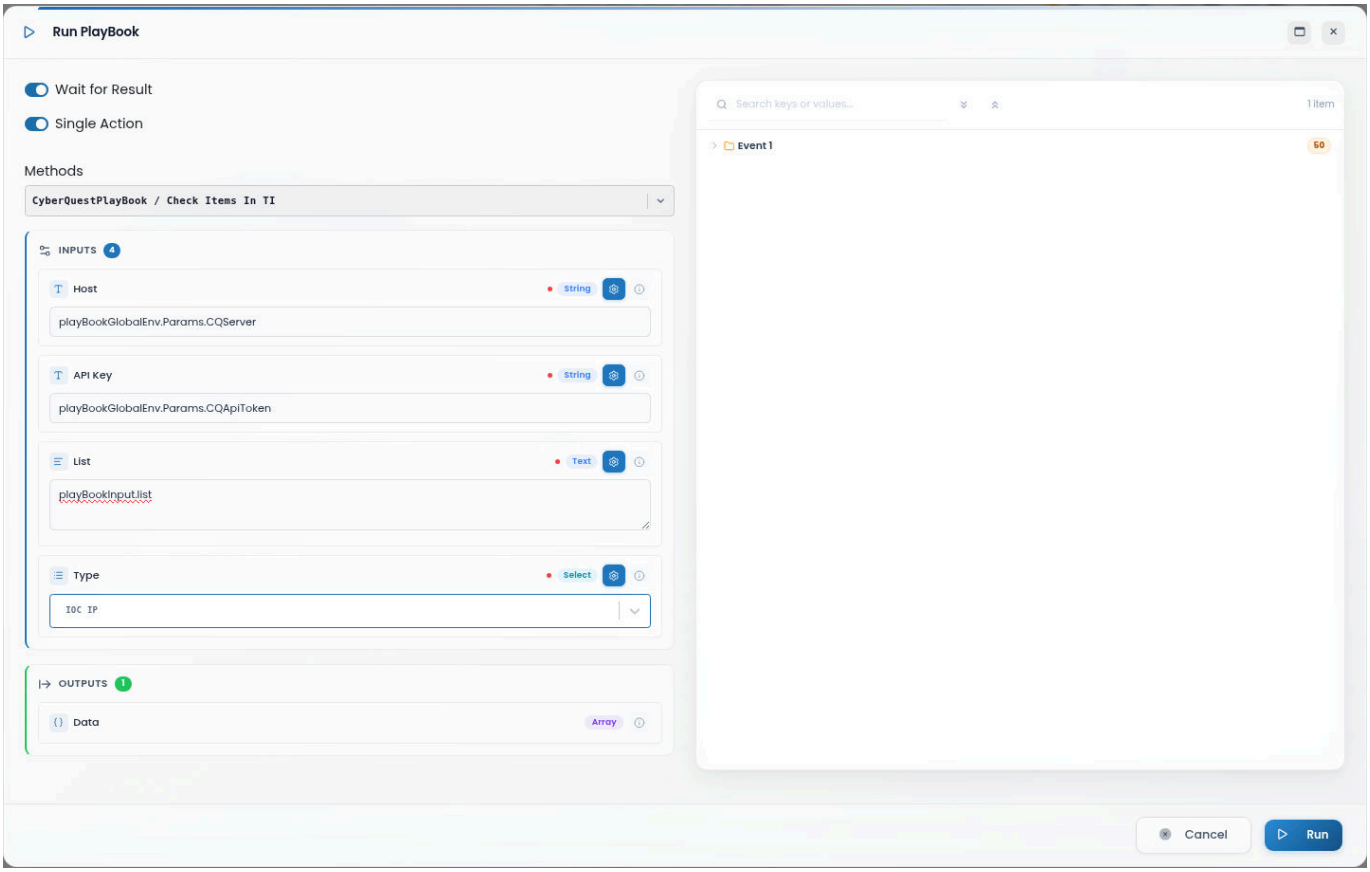
This action is intended to work in a playbook not to be used in a single action.

CyberQuestPlayBook/BreakLoopAfterEnd method

This action is used to stop the ForEachRunPlayBook execution.

CyberQuestPlayBook/Check Items In TI method

Checks a list of IP or Domains or Tor Exit Nodes in Threat Intelligence.

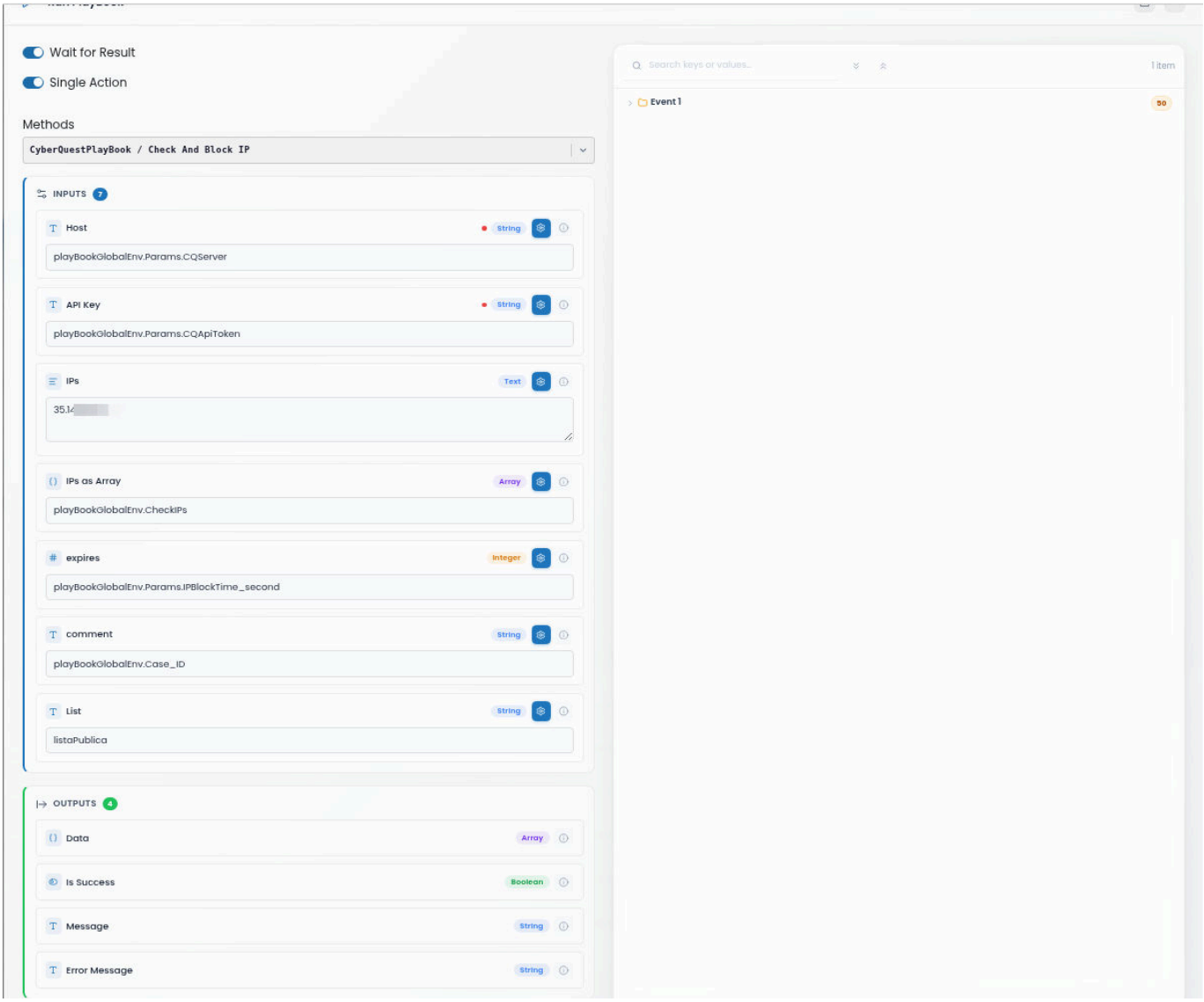


Inputs	Description
Host (is required)	The host of the CQServer
API Key (is required)	The API Key of the CQServer
List (is required)	The list of IPs or Domains or Tor Exit Nodes which will be verified
Type (is required)	The type of check, you can choose from the dropdown list the following items: IPs or Domains or Tor Exit Nodes

Outputs	Description
Data (data)	The results of the API call

CyberQuestPlayBook/Check And Block IP method

Verified whether the IPs are present in the CQTI list, and block them if they are found in that list.

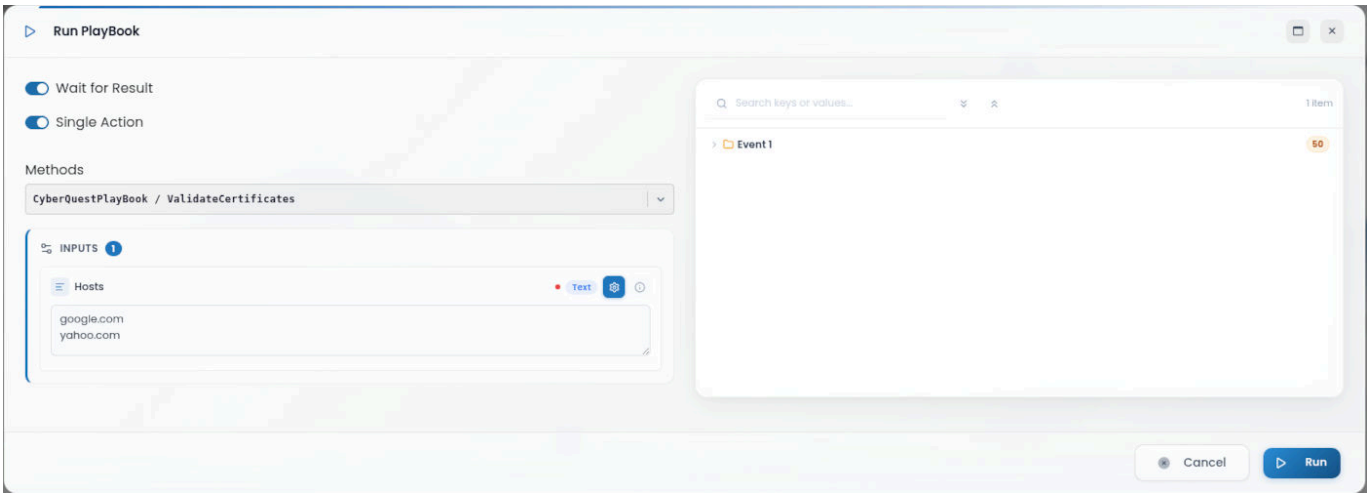


Inputs	Description
Host (is required)	The host of the CQServer
API Key (is required)	The API Key of the CQServer
IPs	A list of the IPs (one per line)
IPs as Array	IPs as Array
expires	The duration of blocking
comment	Additional informations
List	The name of the list

Outputs	Description
Data (data)	The results of the API call
Is Success (isSuccess)	True if the API call is successfull
Message (message)	Additional details of the API call
Error Message (errorMessage)	Additional details of the errors

CyberQuestPlayBook/ValidateCertificates method

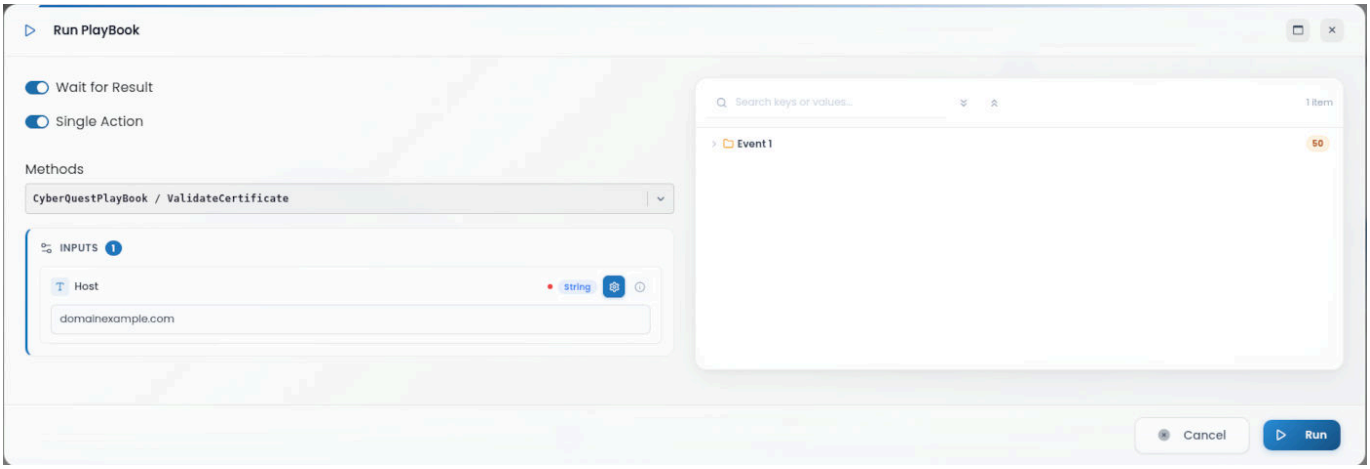
This action is verifying for list of hosts the SSL Certificates.



Inputs	Description
Hosts (is required)	The Hosts you want to check

CyberQuestPlayBook/ValidateCertificate method

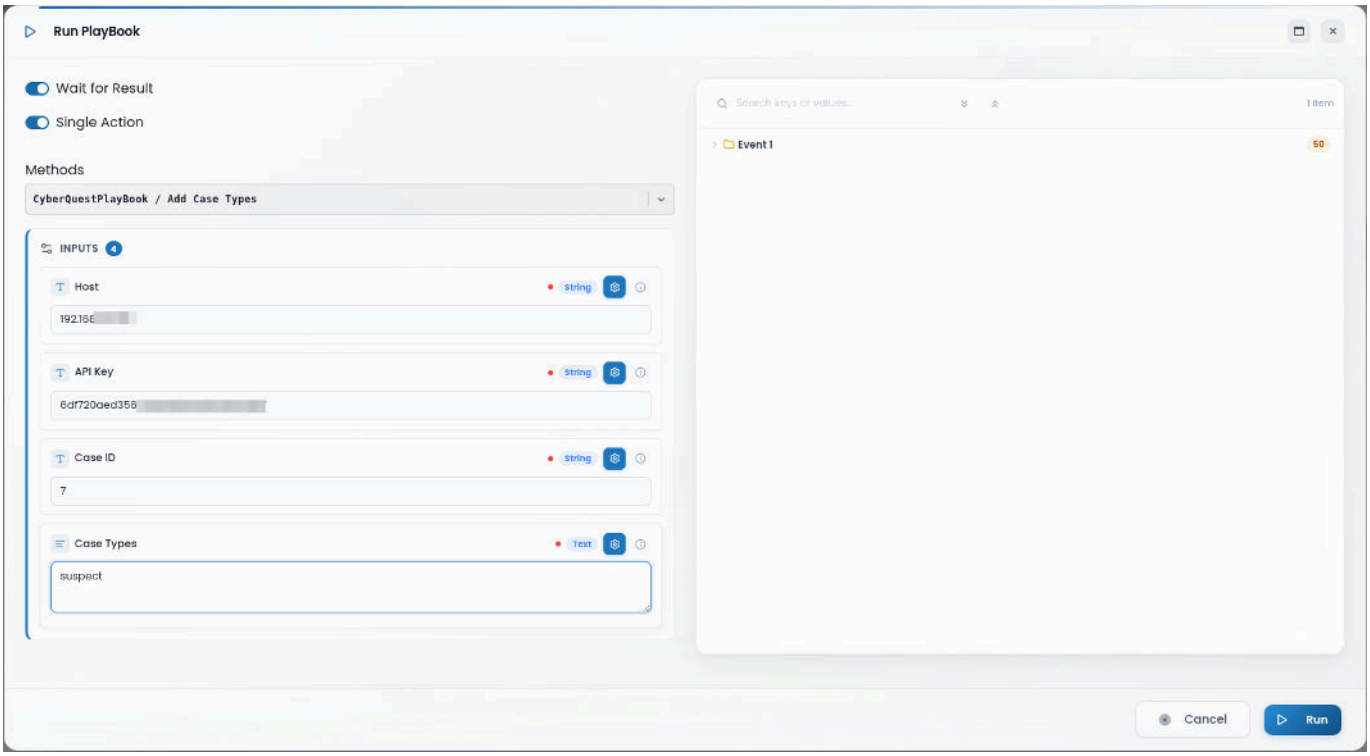
This action is verifying a host the SSL Certificates.



Inputs	Description
Host (is required)	The Host you want to check

CyberQuestPlayBook/Add Case Types method

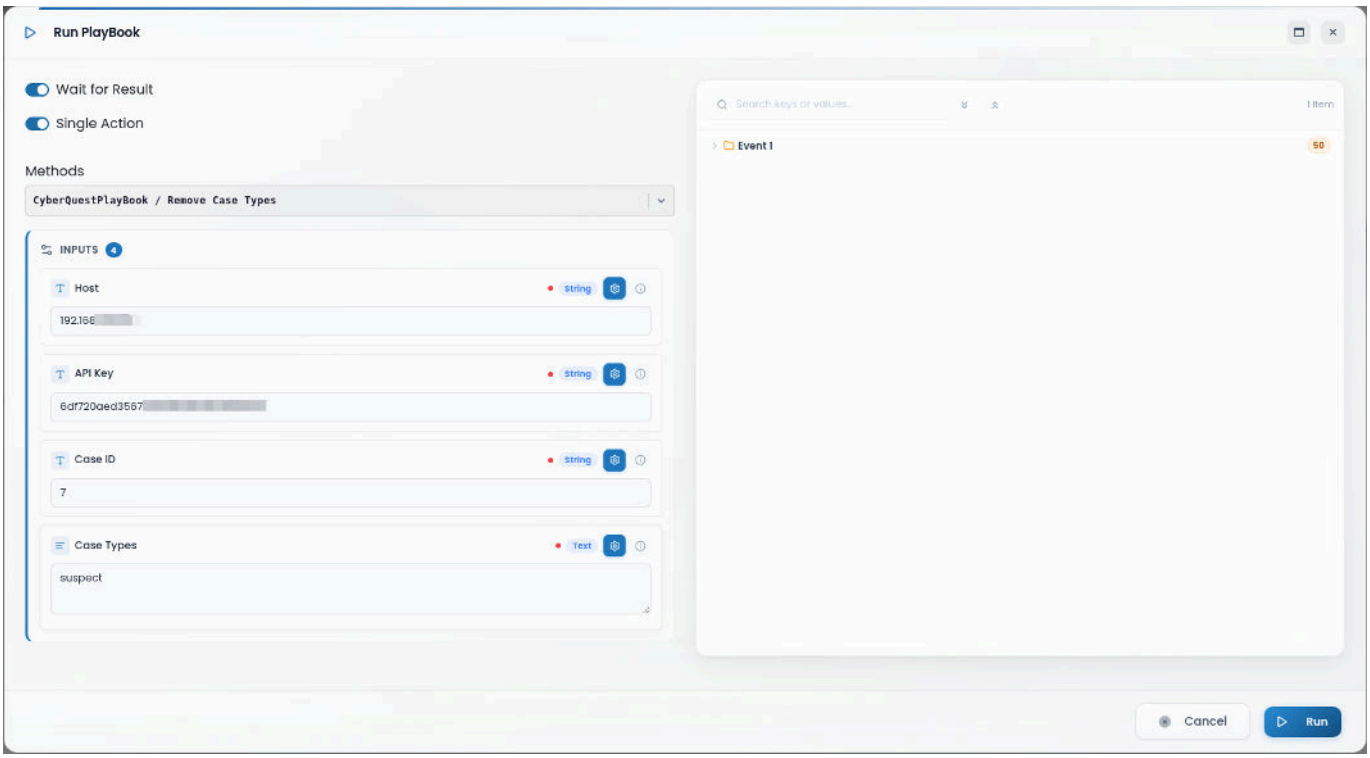
This action is used to add one or more case types to an already open case.



Inputs	Description
Host (is required)	The host of the CQServer
API Key (is required)	The API Key of the CQServer
Case ID (is required)	The Case ID where you wish to assign the case type
Case Types (is required)	The case types which you want to add of the existing case

CyberQuestPlayBook/Remove Case Types method

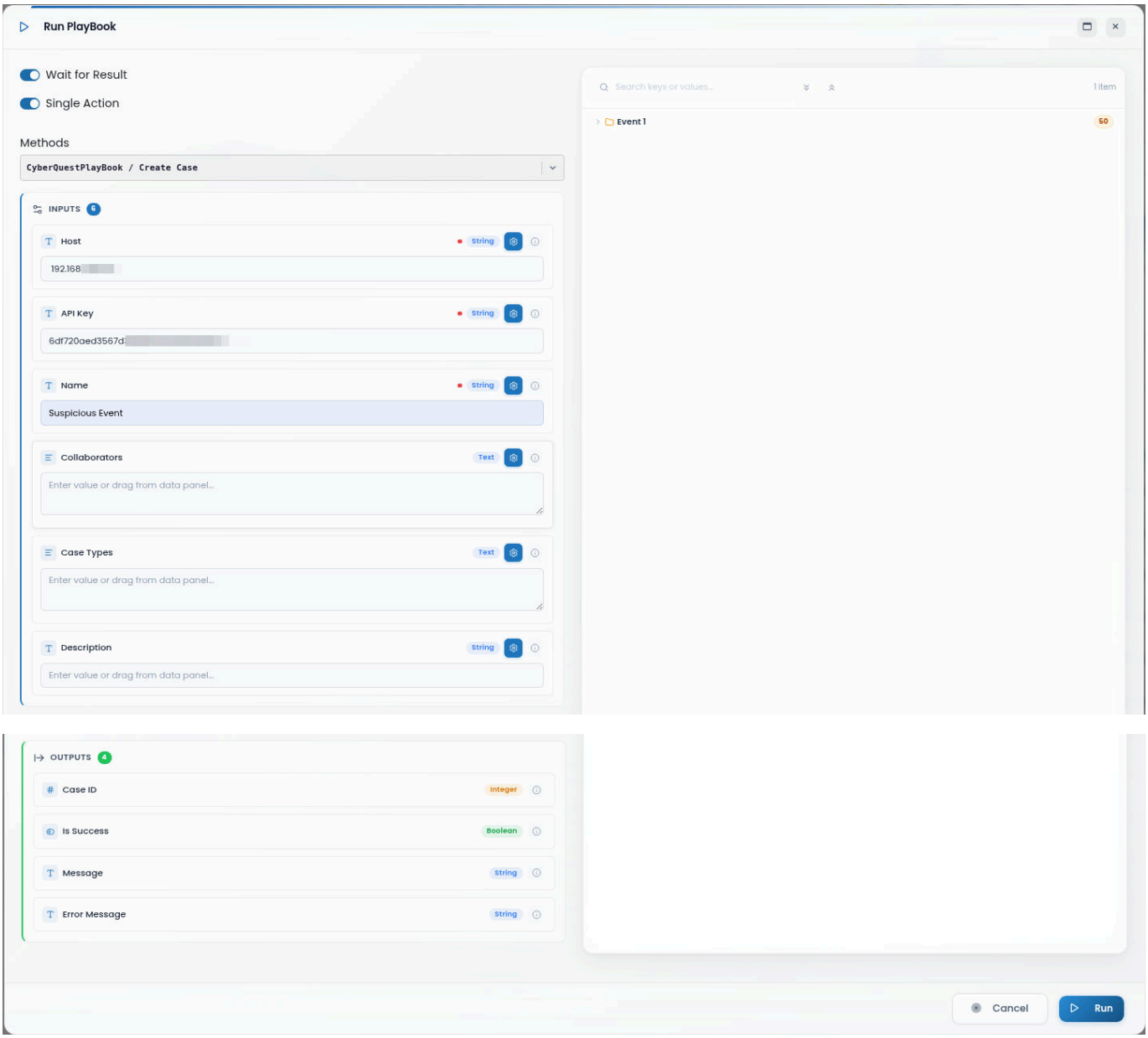
This action is used to remove one or more case types to an already open case.



Inputs	Description
Host (is required)	The host of the CQServer
API Key (is required)	The API Key of the CQServer
Case ID (is required)	The Case ID where you want to delete the case type
Case Types (is required)	The case types which you want to delete of the existing case (one per line)

CyberQuestPlayBook/Create Case method

This action is used to create a new investigation case.

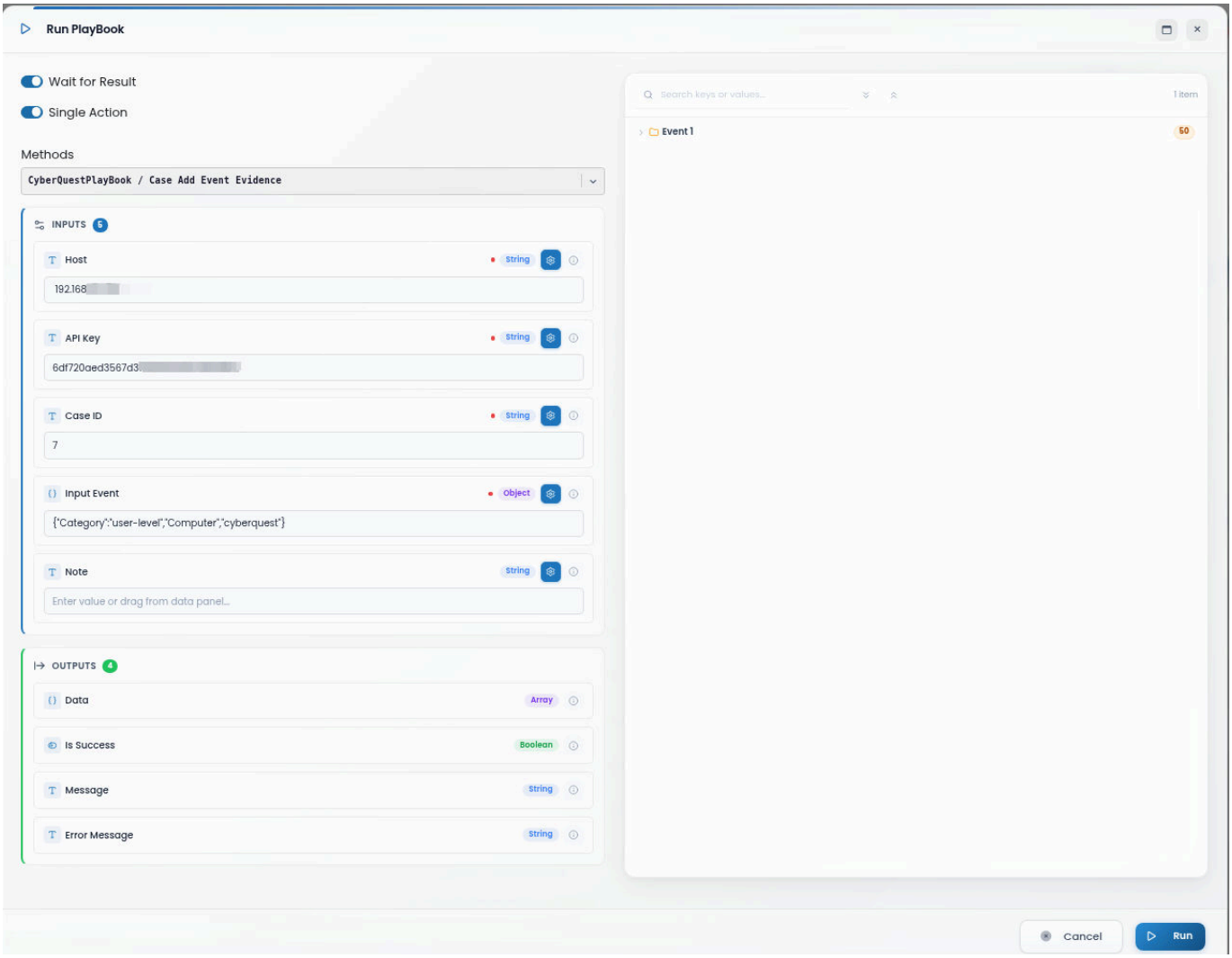


Inputs	Description
Host (is required)	The host of the CQServer
API Key (is required)	The API Key of the CQServer
Name (is required)	The name of the investigation case
Collaborators	A list of users ids that can work on this case (array)
Case Types	A list of case types which you want to add to the investigation case (array of strings)
Description	Additional details about the investigation case.

Outputs	Description
Case ID (case_id)	The ID of the new created investigation case
Is Success (isSuccess)	True if the API call is successfull
Message (message)	Additional details of the API call
Error Message (errorMessage)	Additional details of the errors

CyberQuestPlayBook/Case Add Event Evidence method

This method is used to add additional information (Event) to the existing case.



Inputs	Description
Host (is required)	The host of the CQServer
API Key (is required)	The API Key of the CQServer
Case ID (is required)	The Case ID where you want to add event
Input Event (is required)	Event to be added in the existing case
Note	Additional details about the evidence

Outputs	Description
Data (data)	The results of the API call
Is Success (isSuccess)	True if the API call is successfull
Message (message)	Additional details of the API call
Error Message (errorMessage)	Additional details of the errors

CyberQuestPlayBook/SetKeyValueToGlobalEnv method

Set a variable to be called globally.

Inputs	Description
Key (is required)	The name of the variable
Value (is required)	The value which you want to be stored in variable



This action is intended to work in a playbook not to be used in a single action.

CyberQuestPlayBook/GetKeyValueToGlobalEnv method

This action gets the global parameter.

Inputs	Description
Key (is required)	The name of the variable which is set globally



This action is intended to work in a playbook not to be used in a single action.

CyberQuestPlayBook/Case Add Events method

This method is used to add additional information (Events) to the existing case.

Inputs	Description
Host (is required)	The host of the CQServer
API Key (is required)	The API Key of the CQServer
Case ID (is required)	The Case ID where you want to add events
Input Events (is required)	Events to be added in the existing case
Note	Additional details about the evidence

Outputs	Description
Data (data)	The results of the API call
Is Success (isSuccess)	True if the API call is successfull
Message (message)	Additional details of the API call
Error Message (errorMessage)	Additional details of the errors

CyberQuestPlayBook/Case Add Alert Evidence method

This method is used to add additional information (Alert) to the existing case.

Inputs	Description
Host (is required)	The host of the CQServer
API Key (is required)	The API Key of the CQServer
Case ID (is required)	The Case ID where you want to add alert
Input Alert (is required)	Alert to be added in the existing case
Note	Additional details about the evidence

Outputs	Description
Data (data)	The results of the API call
Is Success (isSuccess)	True if the API call is successfull
Message (message)	Additional details of the API call
Error Message (errorMessage)	Additional details of the errors

CyberQuestPlayBook/Case Add Alerts method

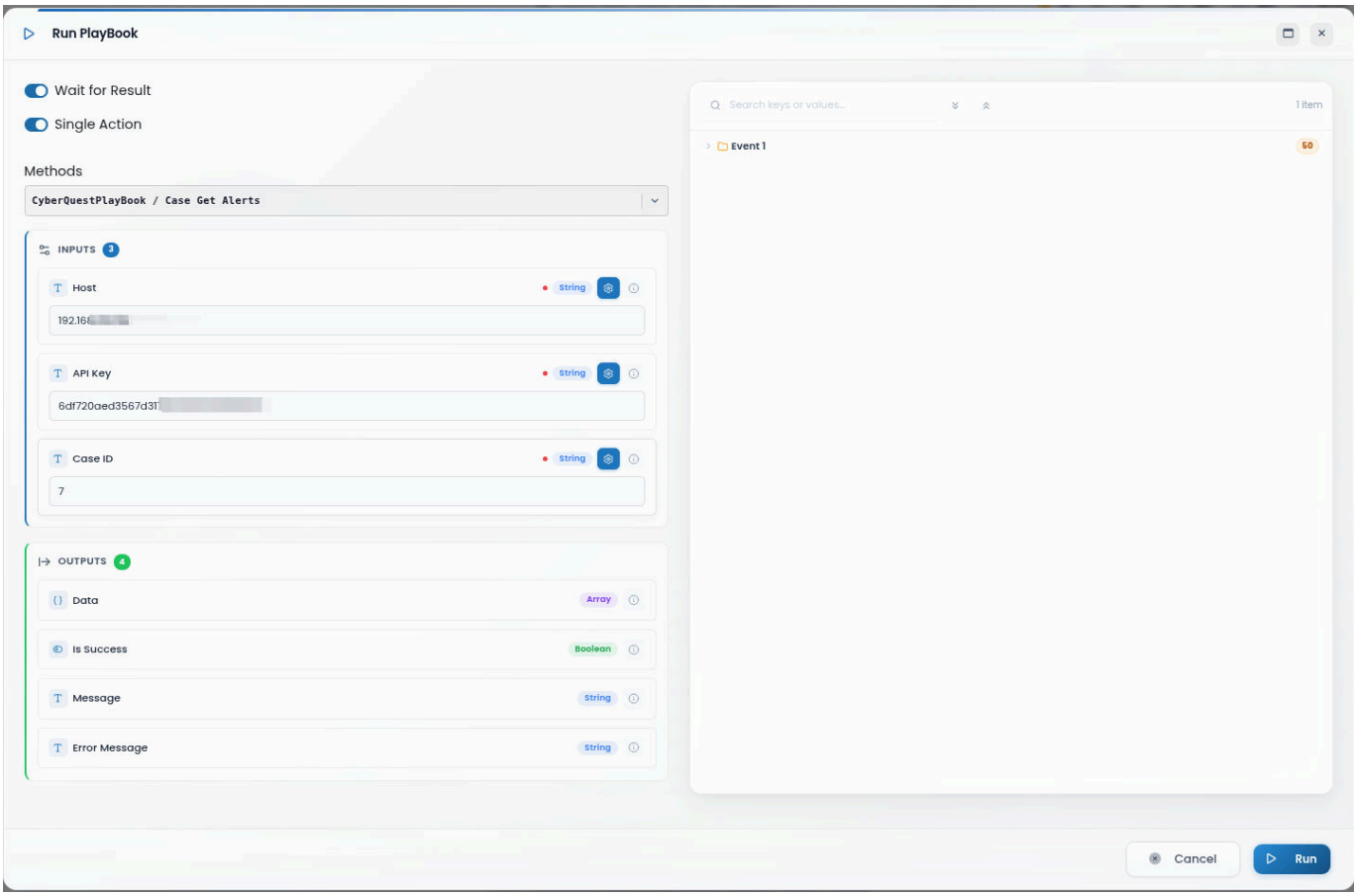
This method is used to add additional information (Alerts) to the existing case.

Inputs	Description
Host (is required)	The host of the CQServer
API Key (is required)	The API Key of the CQServer
Case ID (is required)	The Case ID where you want to add alerts
Input Alerts (is required)	Alerts to be added in the existing case
Note	Additional details about the evidence

Outputs	Description
Data (data)	The results of the API call
Is Success (isSuccess)	True if the API call is successfull
Message (message)	Additional details of the API call
Error Message (errorMessage)	Additional details of the errors

CyberQuestPlayBook/Case Get Alerts method

This method is used to get the alerts from the existing case.

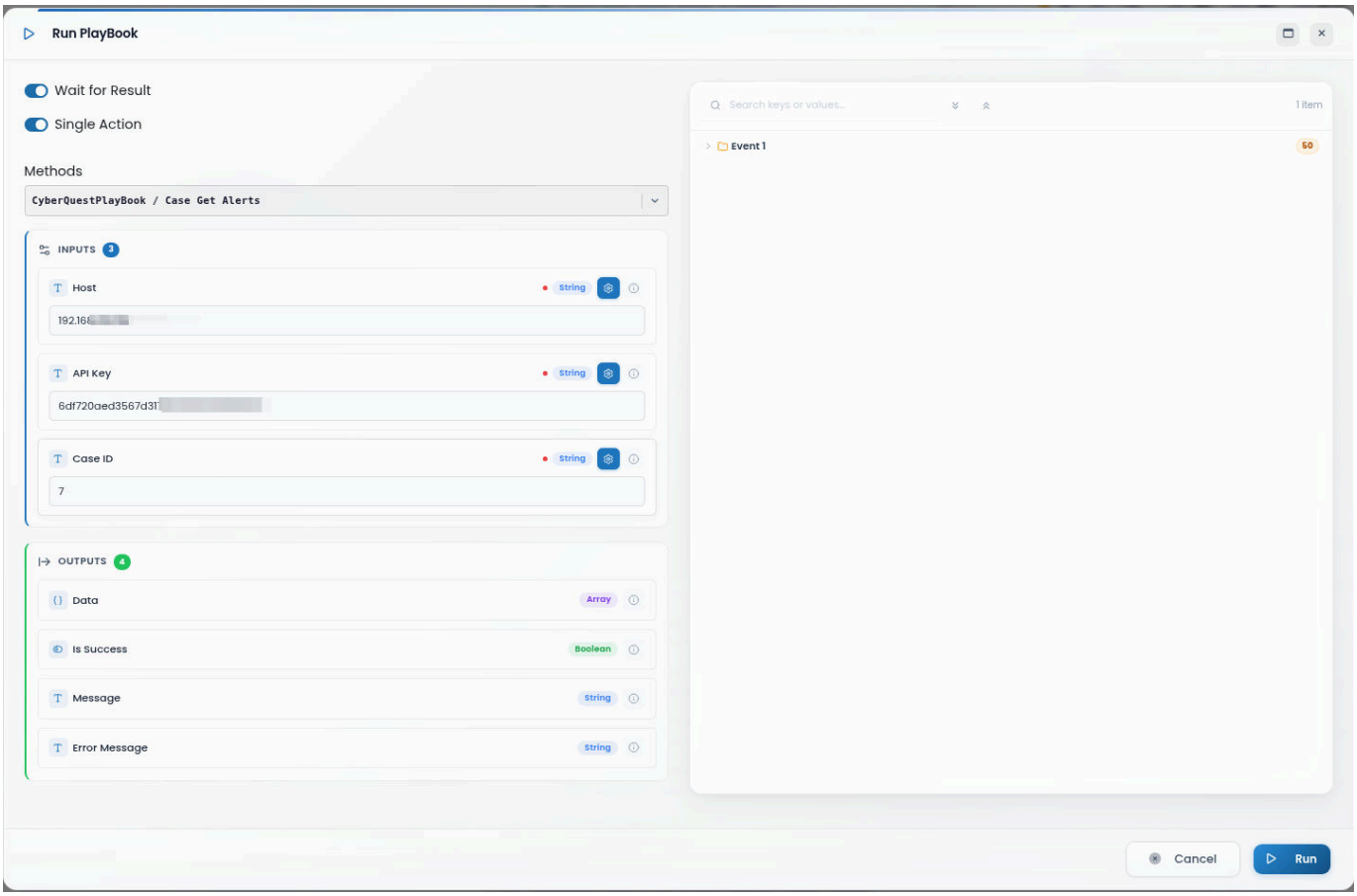


Inputs	Description
Host (is required)	The host of the CQServer
API Key (is required)	The API Key of the CQServer
Case ID (is required)	The Case ID where you want to get the alerts

Outputs	Description
Data (data)	The results of the API call
Is Success (isSuccess)	True if the API call is successfull
Message (message)	Additional details of the API call
Error Message (errorMessage)	Additional details of the errors

CyberQuestPlayBook/Case Get Events method

This method is used to get the events from the existing case.

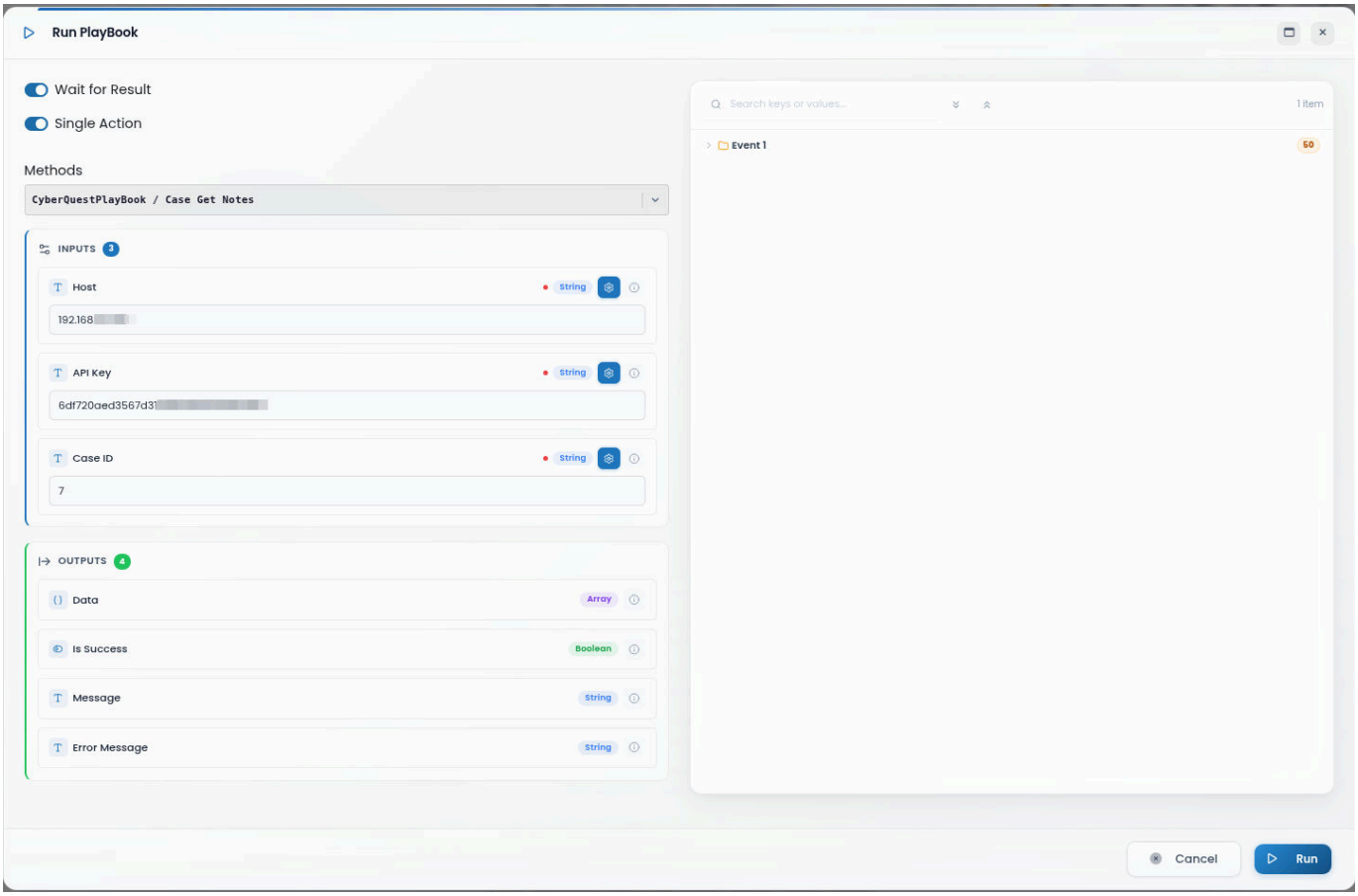


Inputs	Description
Host (is required)	The host of the CQServer
API Key (is required)	The API Key of the CQServer
Case ID (is required)	The Case ID where you want to get the events

Outputs	Description
Data (data)	The results of the API call
Is Success (isSuccess)	True if the API call is successfull
Message (message)	Additional details of the API call
Error Message (errorMessage)	Additional details of the errors

CyberQuestPlayBook/Case Get Notes method

This method is used to get the notes from the existing case.

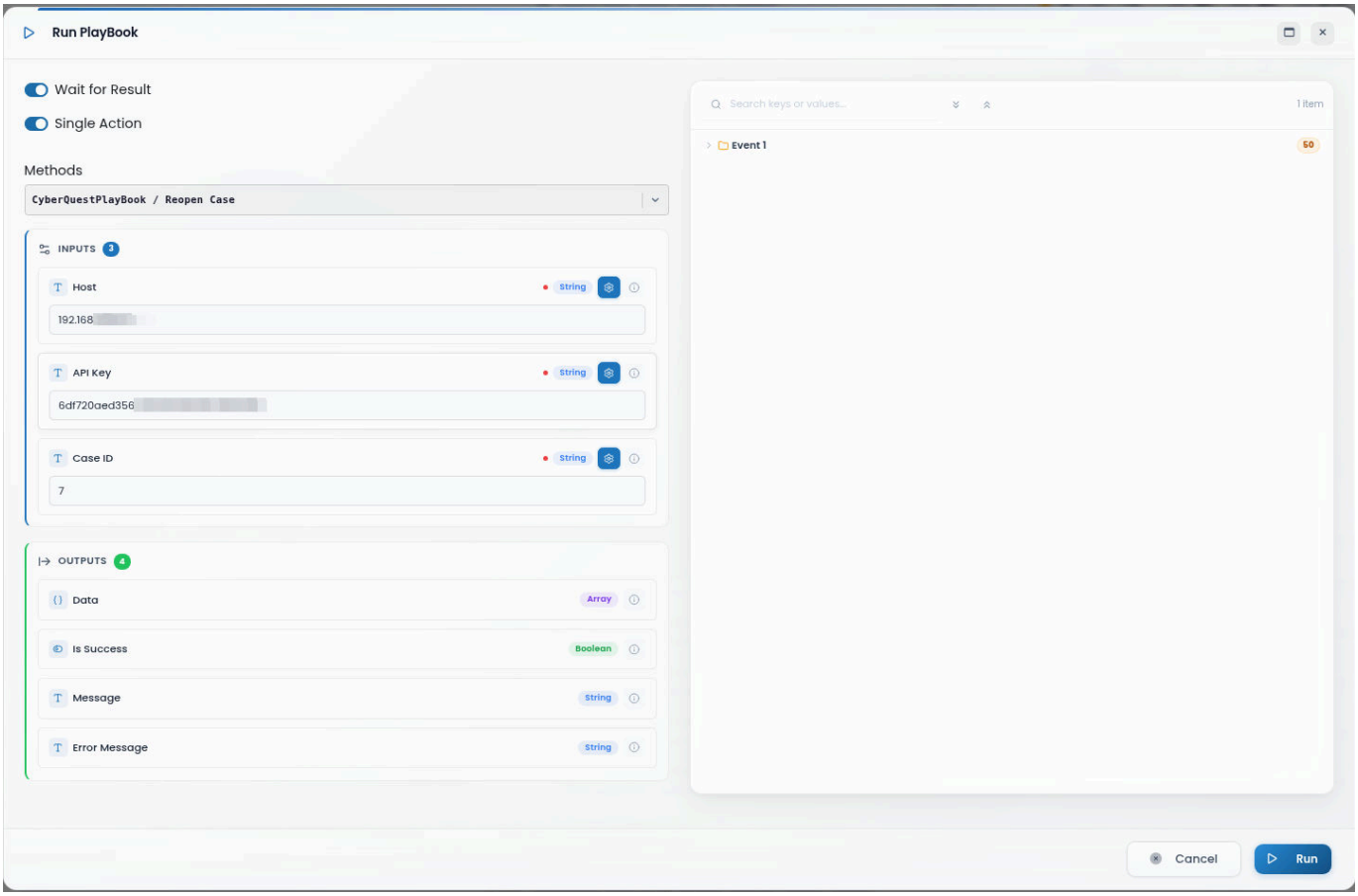


Inputs	Description
Host (is required)	The host of the CQServer
API Key (is required)	The API Key of the CQServer
Case ID (is required)	The Case ID where you want to get the notes

Outputs	Description
Data (data)	The results of the API call
Is Success (isSuccess)	True if the API call is successfull
Message (message)	Additional details of the API call
Error Message (errorMessage)	Additional details of the errors

CyberQuestPlayBook/Reopen Case method

This method is used to reopen the case which were closed.

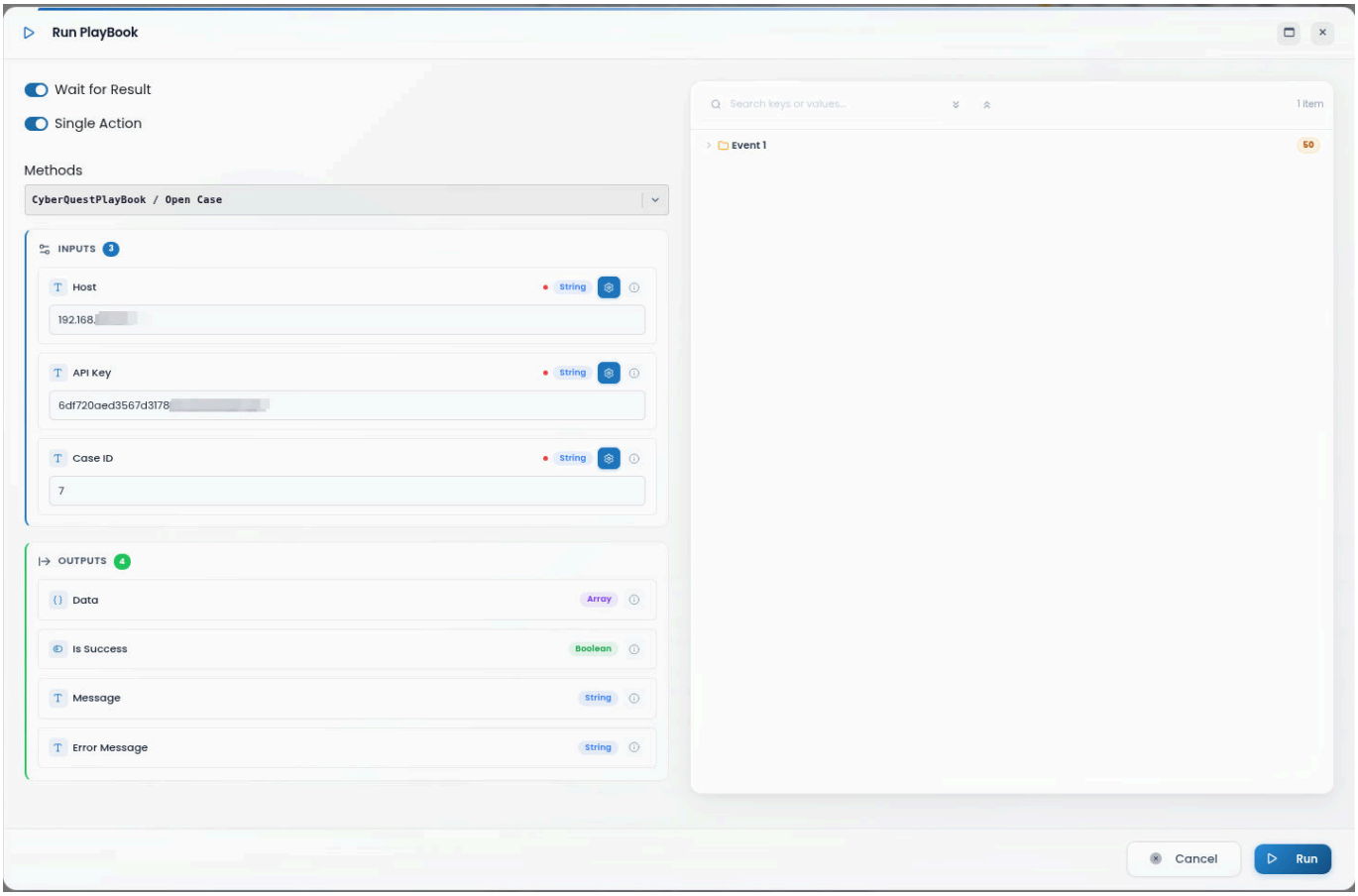


Inputs	Description
Host (is required)	The host of the CQServer
API Key (is required)	The API Key of the CQServer
Case ID (is required)	The Case ID of the case which you want to reopen

Outputs	Description
Data (data)	The results of the API call
Is Success (isSuccess)	True if the API call is successfull
Message (message)	Additional details of the API call
Error Message (errorMessage)	Additional details of the errors

CyberQuestPlayBook/Open Case method

This action help to classify the open cases.

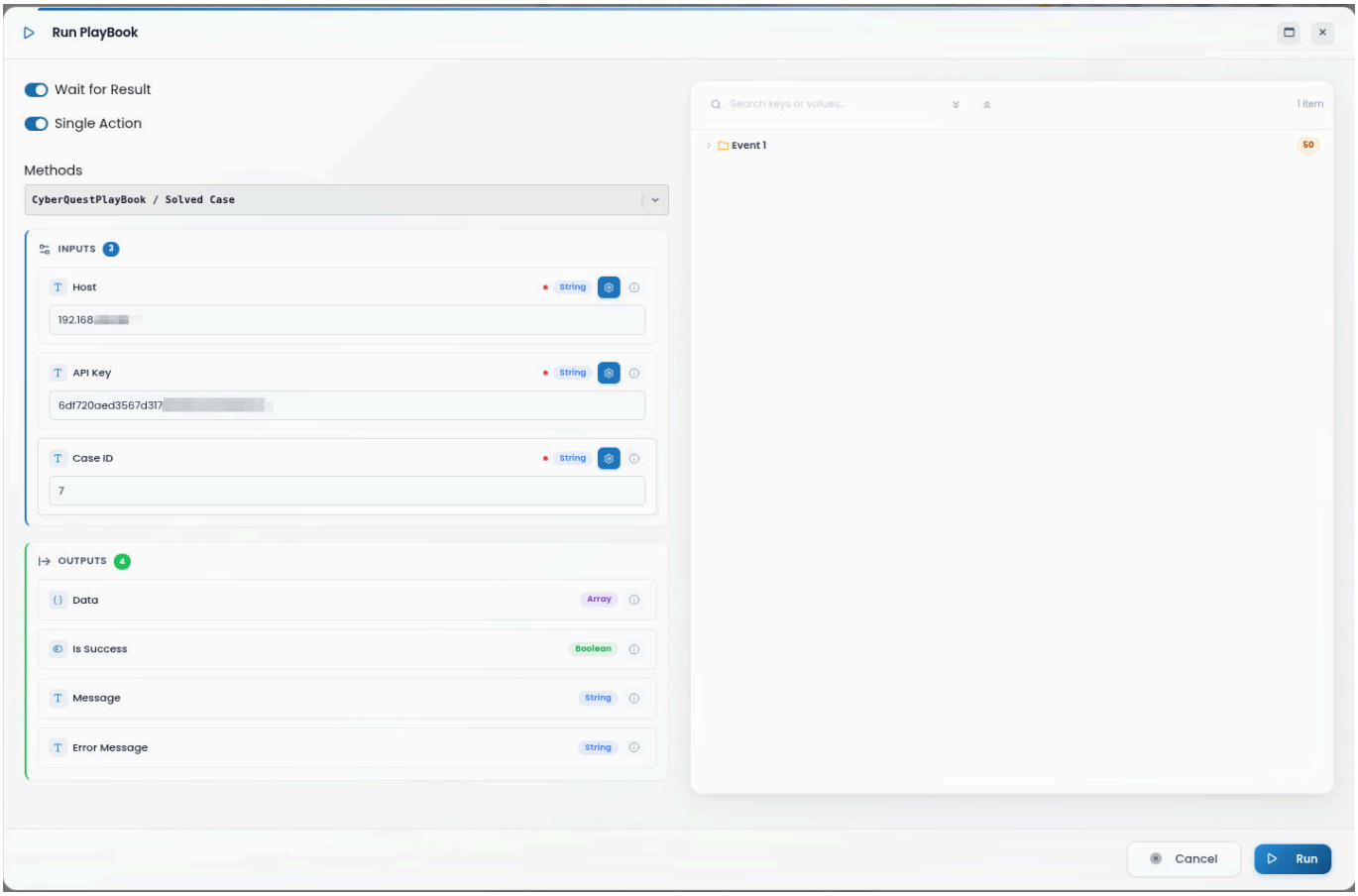


Inputs	Description
Host (is required)	The host of the CQServer
API Key (is required)	The API Key of the CQServer
Case ID (is required)	The Case ID of the case which you want to classify

Outputs	Description
Data (data)	The results of the API call
Is Success (isSuccess)	True if the API call is successfull
Message (message)	Additional details of the API call
Error Message (errorMessage)	Additional details of the errors

CyberQuestPlayBook/Solved Case method

This action help to classify the solved cases.

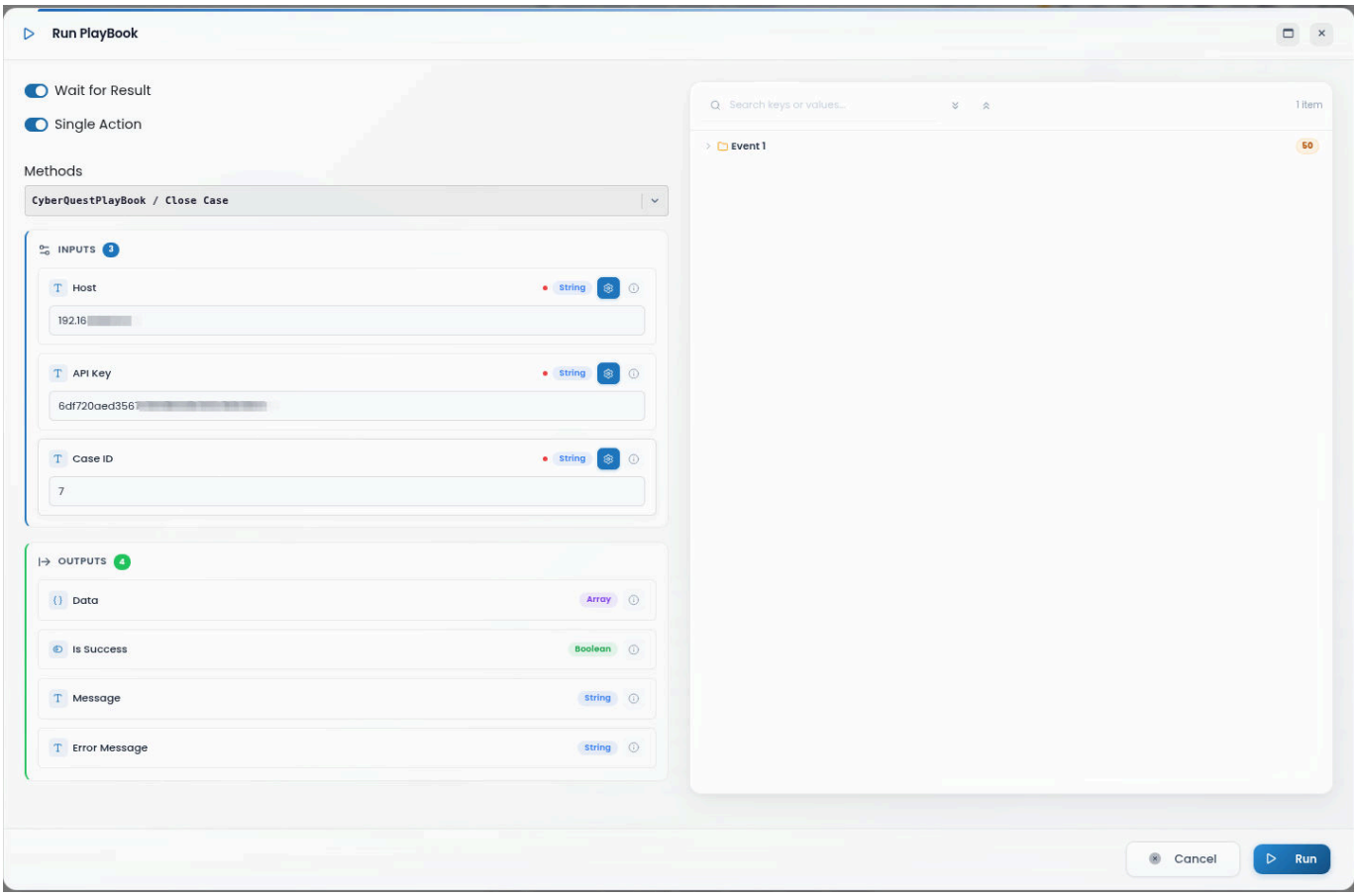


Inputs	Description
Host (is required)	The host of the CQServer
API Key (is required)	The API Key of the CQServer
Case ID (is required)	The Case ID of the case which you want to classify

Outputs	Description
Data (data)	The results of the API call
Is Success (isSuccess)	True if the API call is successfull
Message (message)	Additional details of the API call
Error Message (errorMessage)	Additional details of the errors

CyberQuestPlayBook/Close Case method

This action help to classify the closed cases.

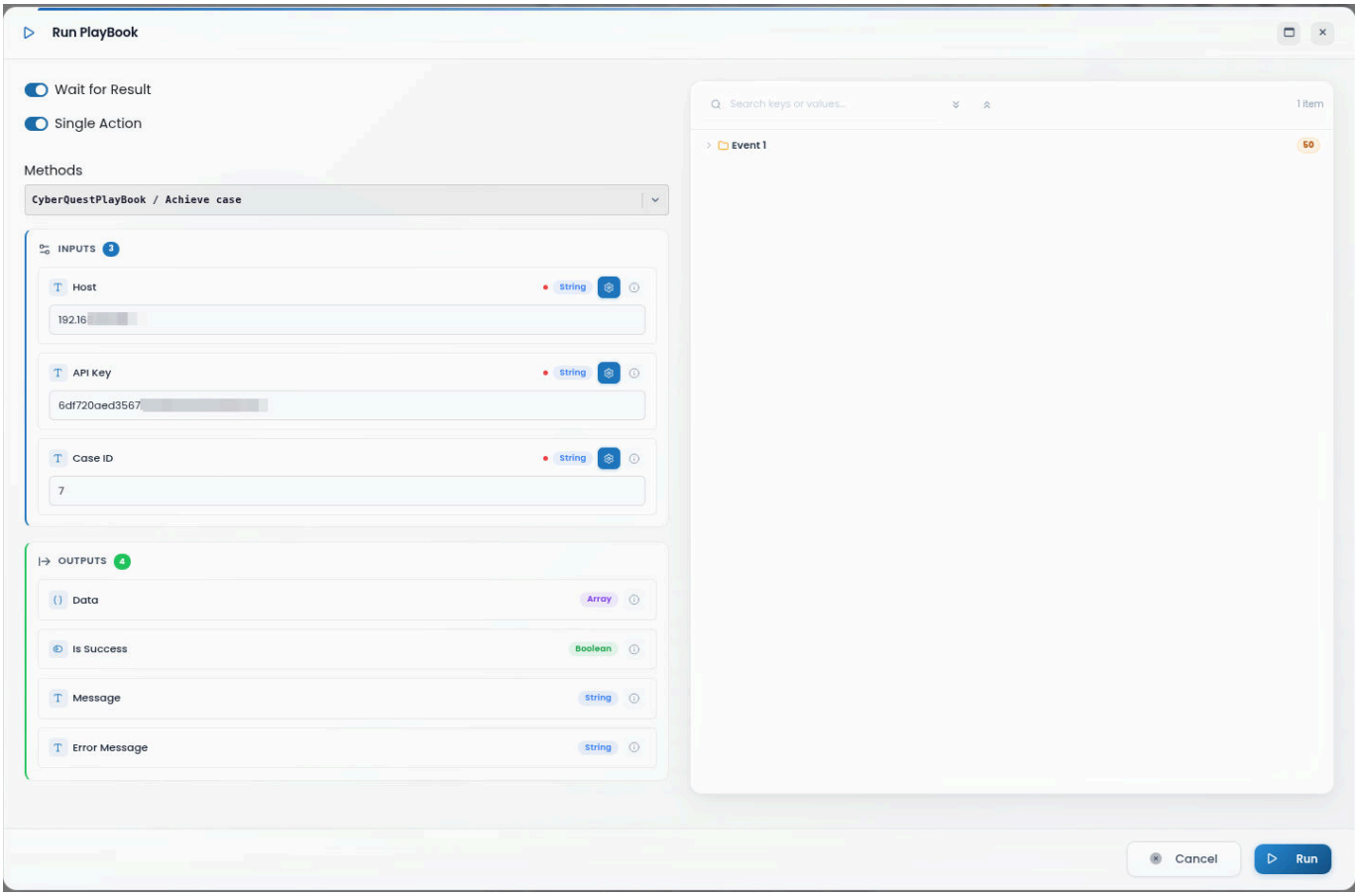


Inputs	Description
Host (is required)	The host of the CQServer
API Key (is required)	The API Key of the CQServer
Case ID (is required)	The Case ID of the case which you want to classify

Outputs	Description
Data (data)	The results of the API call
Is Success (isSuccess)	True if the API call is successfull
Message (message)	Additional details of the API call
Error Message (errorMessage)	Additional details of the errors

CyberQuestPlayBook/Achieve case method

This action help to archive the cases.

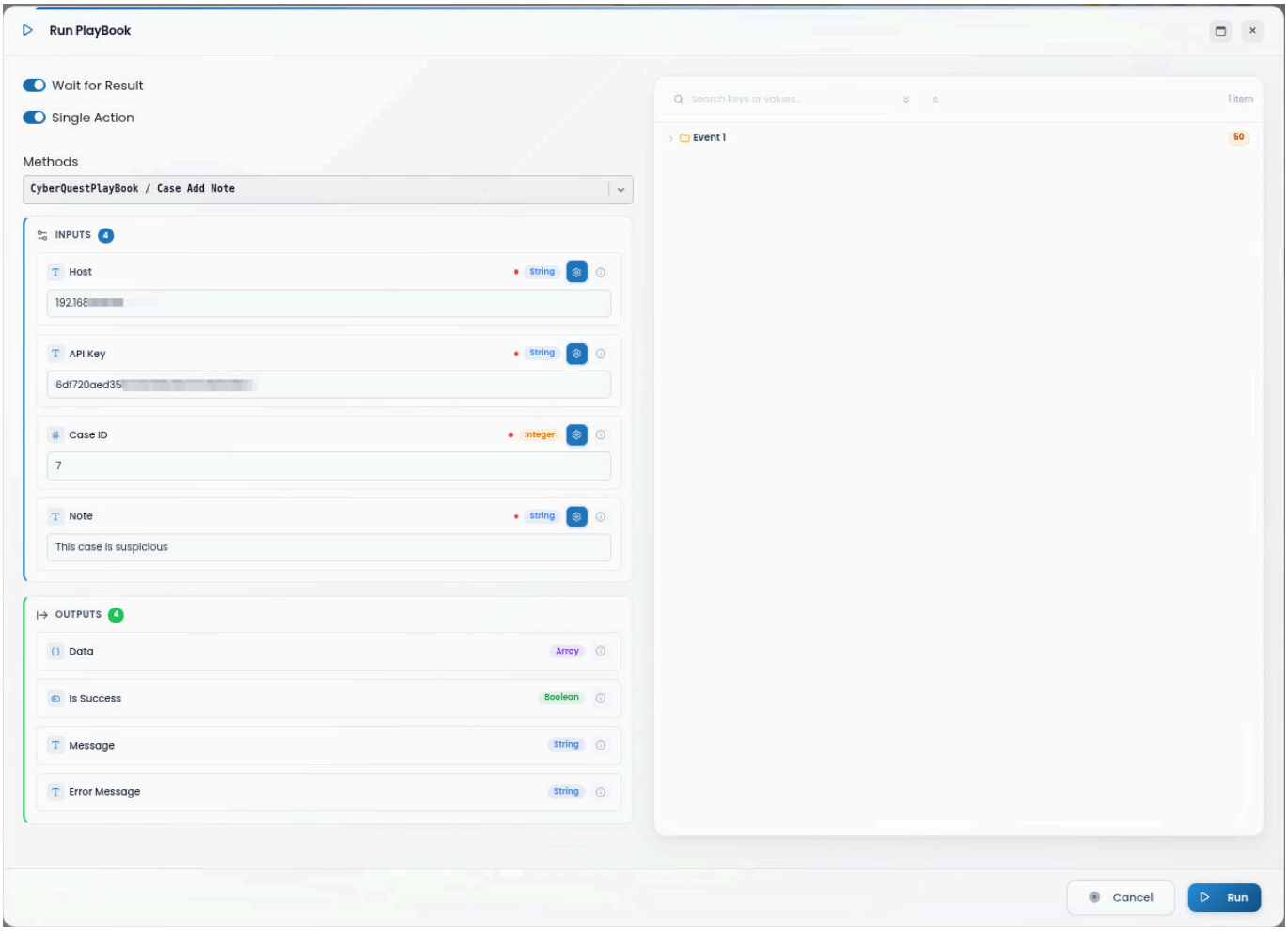


Inputs	Description
Host (is required)	The host of the CQServer
API Key (is required)	The API Key of the CQServer
Case ID (is required)	The Case ID of the case which you want to archive

Outputs	Description
Data (data)	The results of the API call
Is Success (isSuccess)	True if the API call is successfull
Message (message)	Additional details of the API call
Error Message (errorMessage)	Additional details of the errors

CyberQuestPlayBook/Case Add Note method

This action help to create a note for the existing cases.

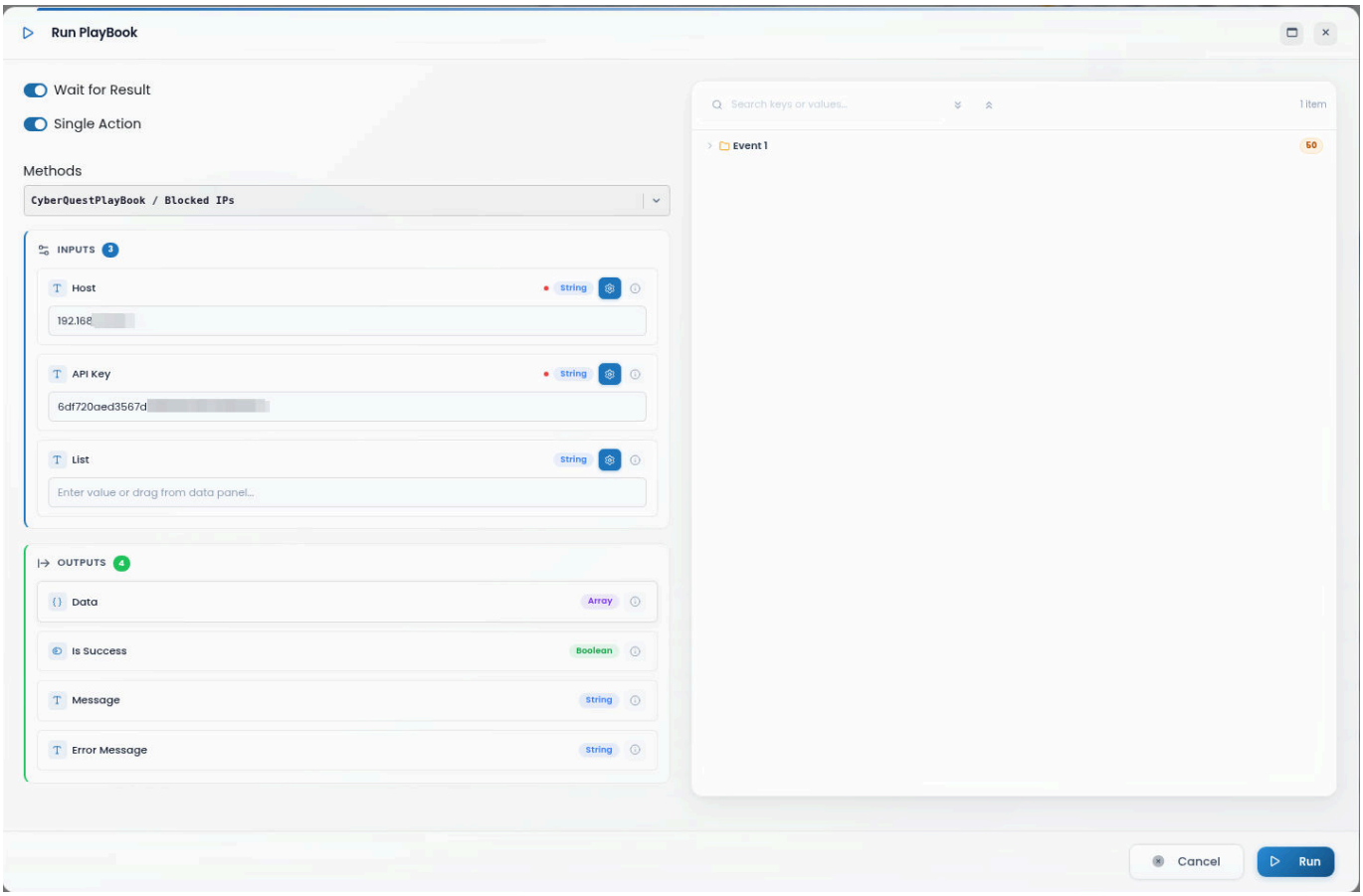


Inputs	Description
Host (is required)	The host of the CQServer
API Key (is required)	The API Key of the CQServer
Case ID (is required)	The Case ID of the existing case which you want to add the note
Note (is required)	The informations you want to add to the Note

Outputs	Description
Data (data)	The results of the API call
Is Success (isSuccess)	True if the API call is successfull
Message (message)	Additional details of the API call
Error Message (errorMessage)	Additional details of the errors

CyberQuestPlayBook/Blocked IPs method

This method help you to block a list of IPs.

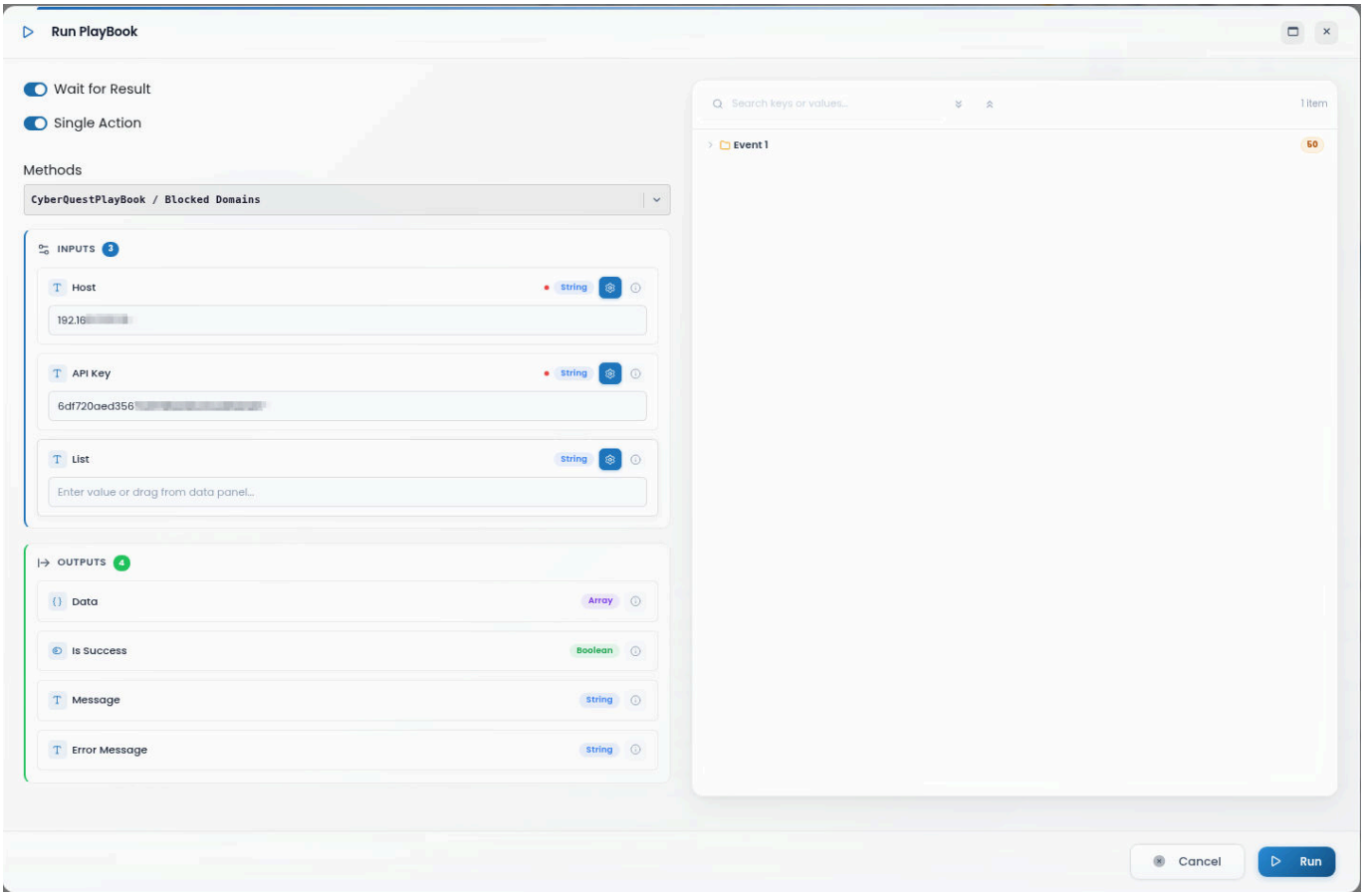


Inputs	Description
Host (is required)	The host of the CQServer
API Key (is required)	The API Key of the CQServer
List	The list of IPs that you want to block

Outputs	Description
Data (data)	The results of the API call
Is Success (isSuccess)	True if the API call is successfull
Message (message)	Additional details of the API call
Error Message (errorMessage)	Additional details of the errors

CyberQuestPlayBook/Blocked Domains method

This method help you to block a list of Domains.

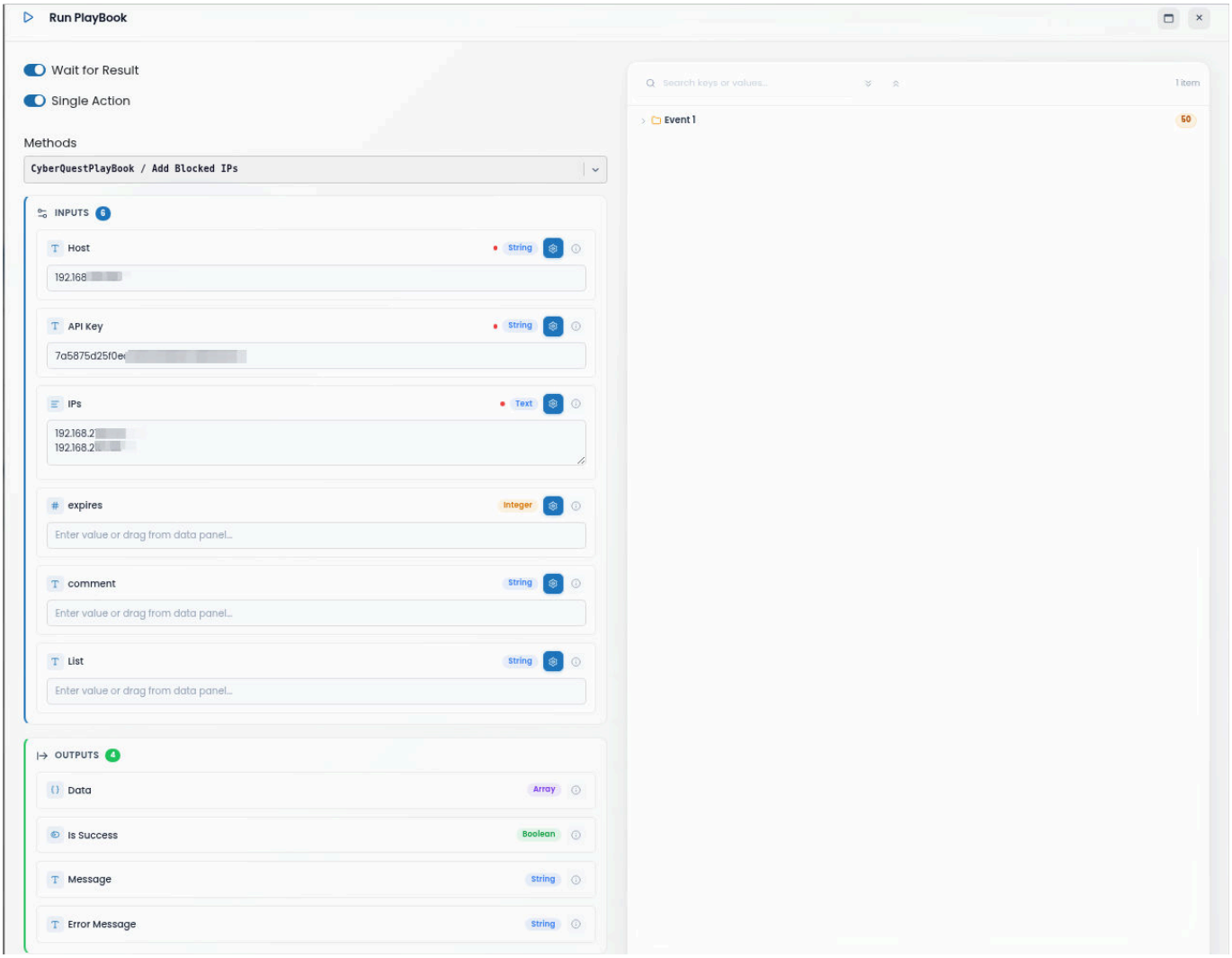


Inputs	Description
Host (is required)	The host of the CQServer
API Key (is required)	The API Key of the CQServer
List	The list of Domains that you want to block

Outputs	Description
Data (data)	The results of the API call
Is Success (isSuccess)	True if the API call is successfull
Message (message)	Additional details of the API call
Error Message (errorMessage)	Additional details of the errors

CyberQuestPlayBook/Add Blocked IPs method

This action help you to block a list o IPs.

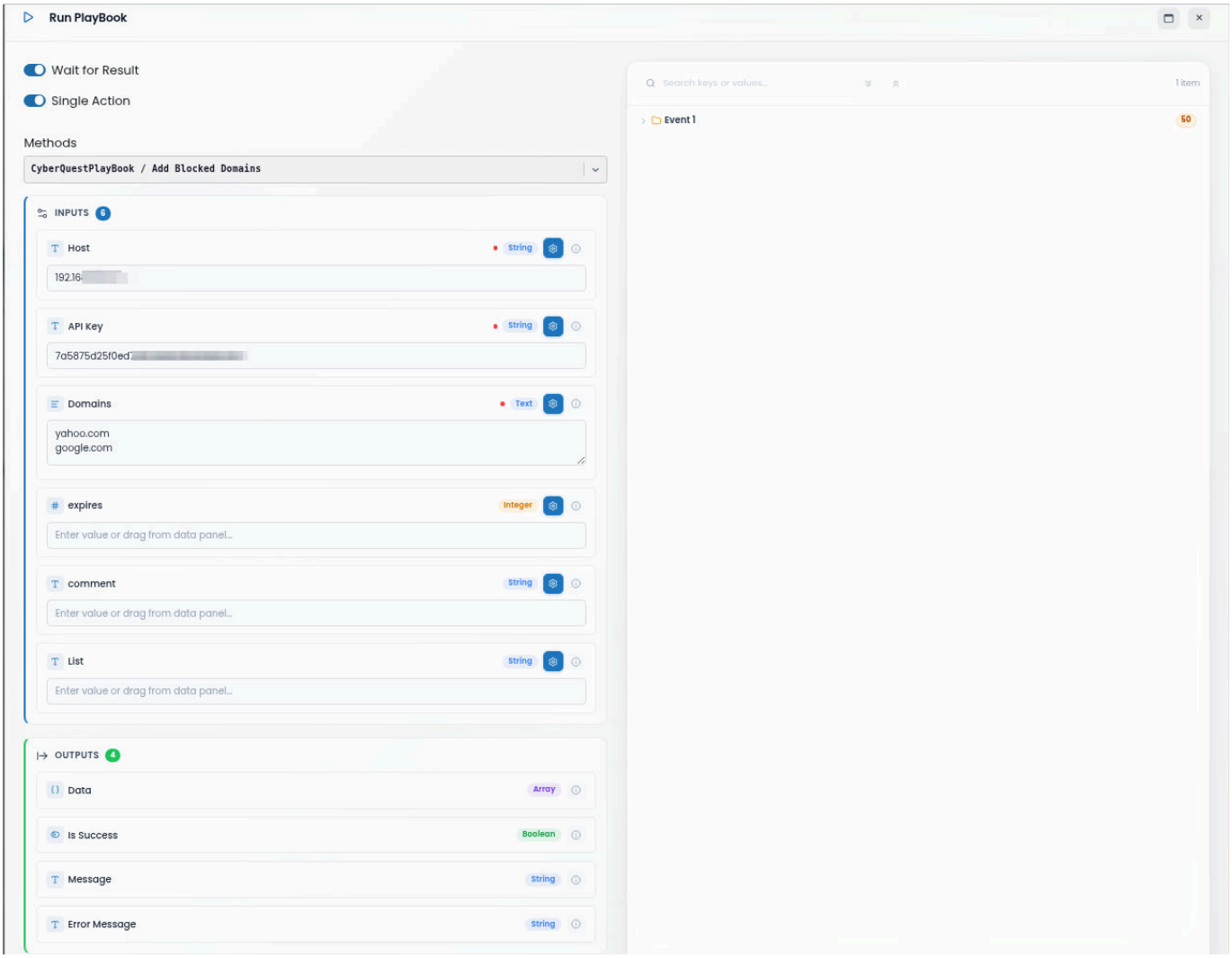


Inputs	Description
Host (is required)	The host of the CQServer
API Key (is required)	The API Key of the CQServer
IPs (is required)	A list of the IPs (one per line)
expires	The duration of blocking
comment	Additional informations
List	The name of the list

Outputs	Description
Data (data)	The results of the API call
Is Success (isSuccess)	True if the API call is successfull
Message (message)	Additional details of the API call
Error Message (errorMessage)	Additional details of the errors

CyberQuestPlayBook/Add Blocked Domains method

This action help you to block a list o Domains.

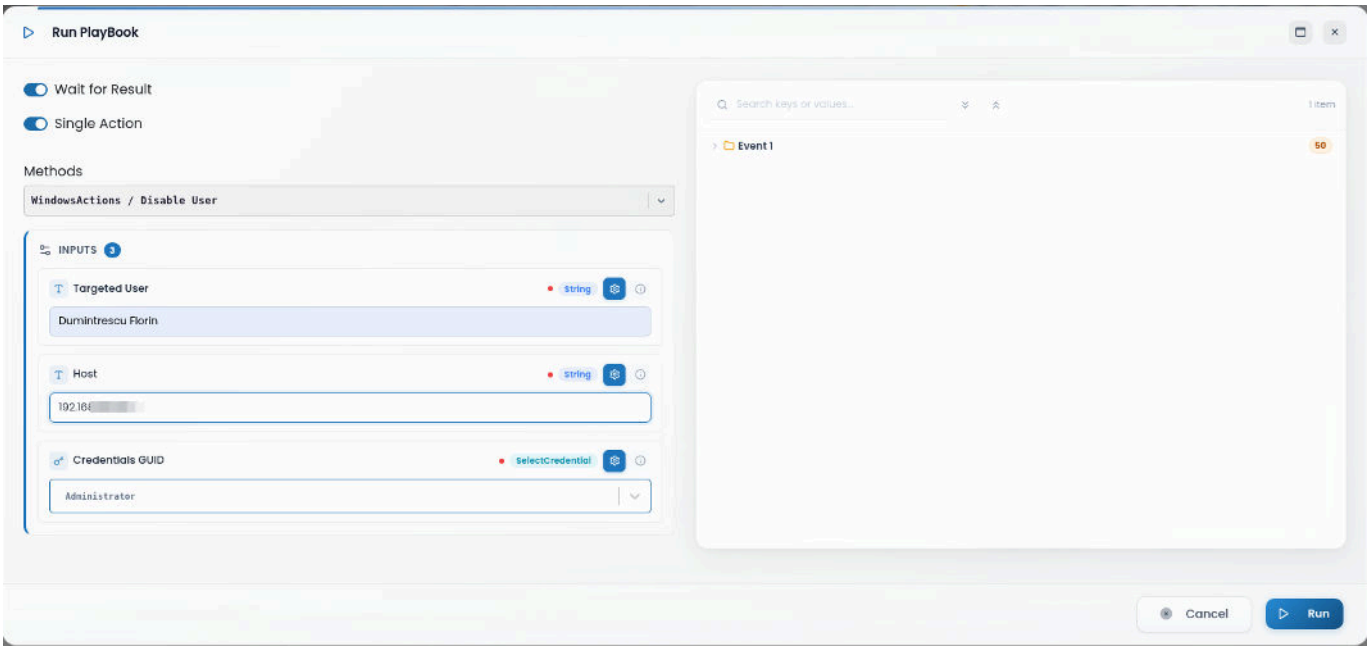


Inputs	Description
Host (is required)	The host of the CQServer
API Key (is required)	The API Key of the CQServer
Domains (is required)	A list of the Domains (one per line)
expires	The duration of blocking
comment	Additional informations
List	The name of the list

Outputs	Description
Data (data)	The results of the API call
Is Success (isSuccess)	True if the API call is successfull
Message (message)	Additional details of the API call
Error Message (errorMessage)	Additional details of the errors

LinuxActions/Disable User method

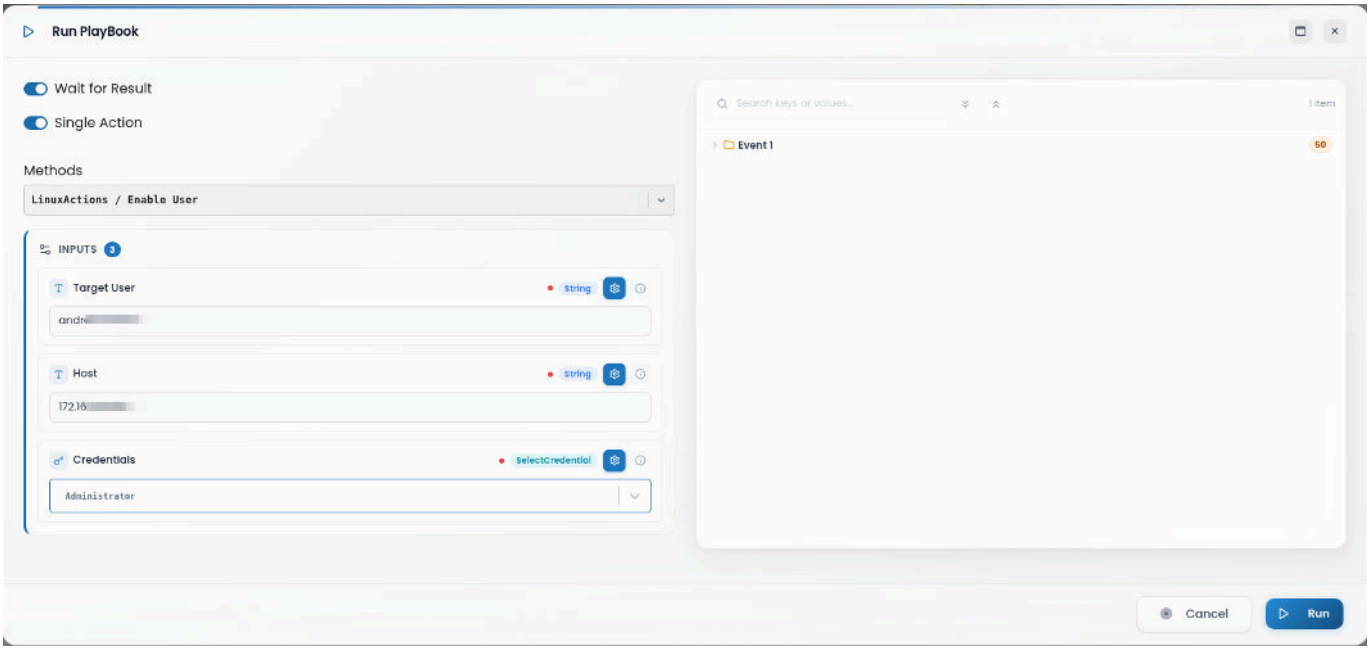
This action is used to Disable a User.



Inputs	Description
Target User (is required)	The user who is targeted
Host (is required)	The target host
Credentials (is required)	The credentials of the Computer that you want to disable

LinuxActions/Enable User method

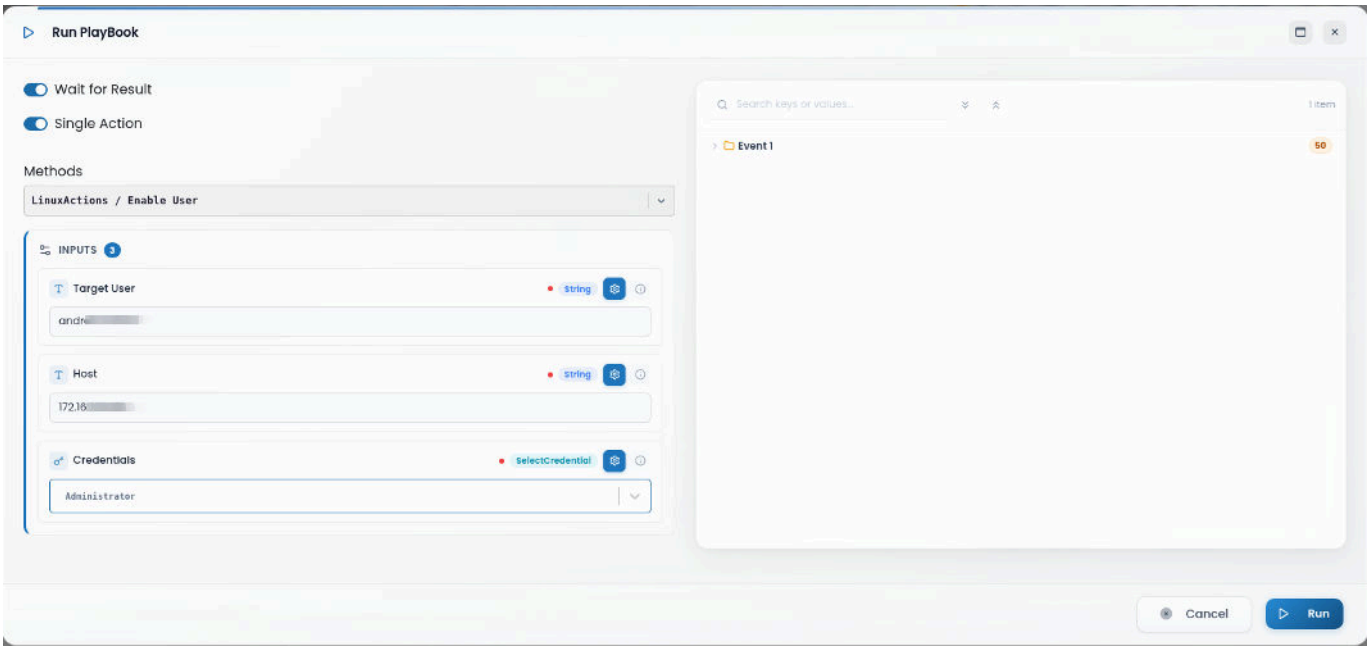
This action is used to Enable a User.



Inputs	Description
Target User (is required)	The user who is targeted
Host (is required)	The target host
Credentials (is required)	The credentials of the Computer that you want to enable

LinuxActions/Expire User Password method

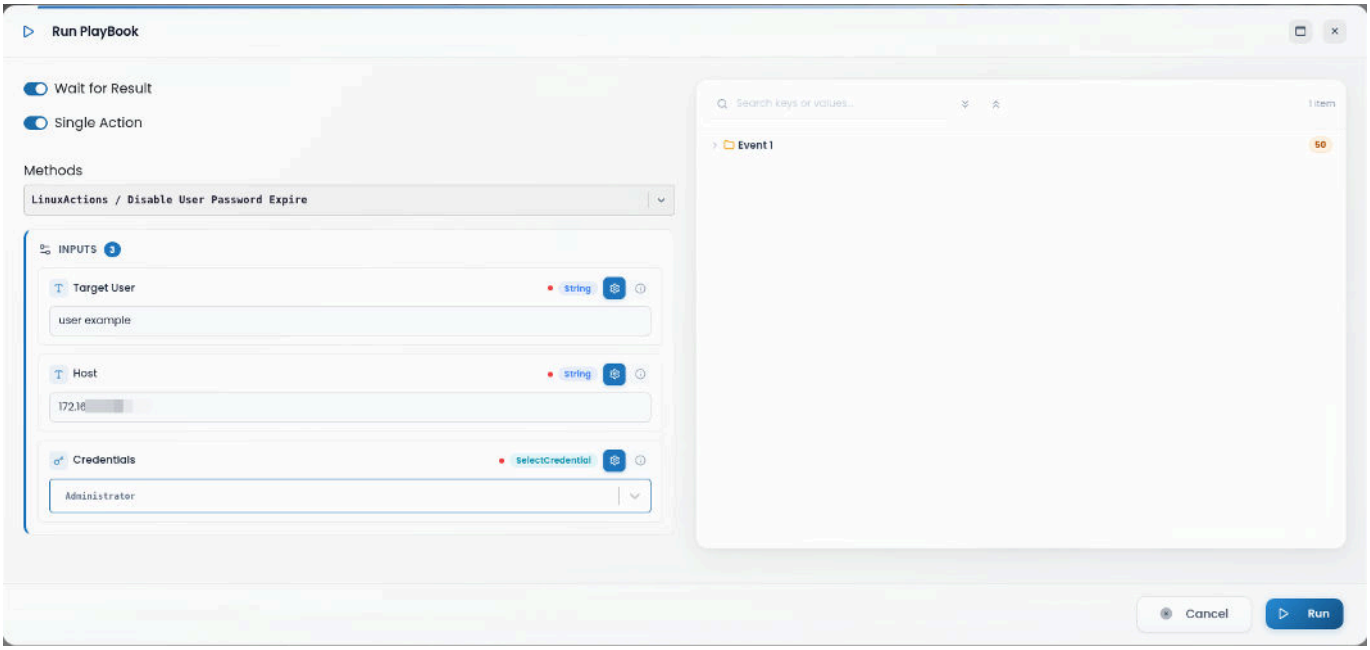
This action is used to set the period of the User password.



Inputs	Description
Target User (is required)	The user who is targeted
Host (is required)	The target host
Credentials (is required)	The credentials of the Computer that you want to set the period of the password

LinuxActions/Disable User Password Expire method

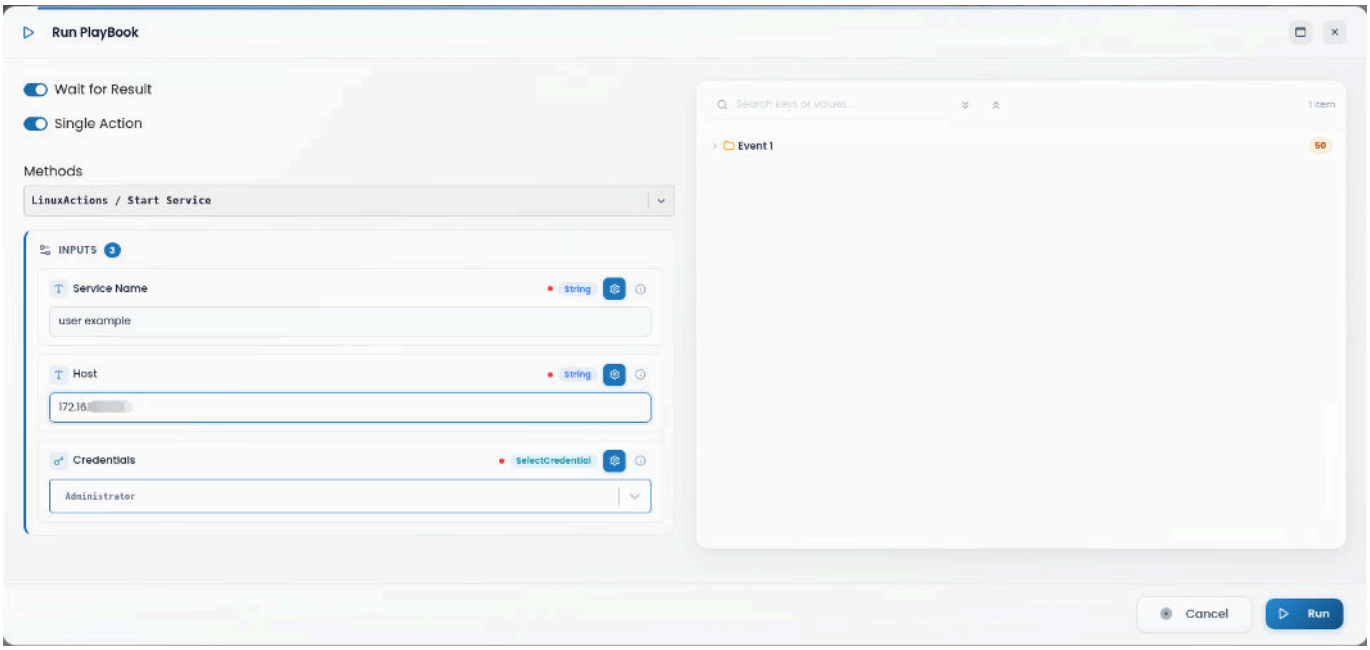
This action is used to disable the period of the User password.



Inputs	Description
Target User (is required)	The user who is targeted
Host (is required)	The target host
Credentials (is required)	The credentials of the Computer that you want to disable the period of the password

LinuxActions/Start Service method

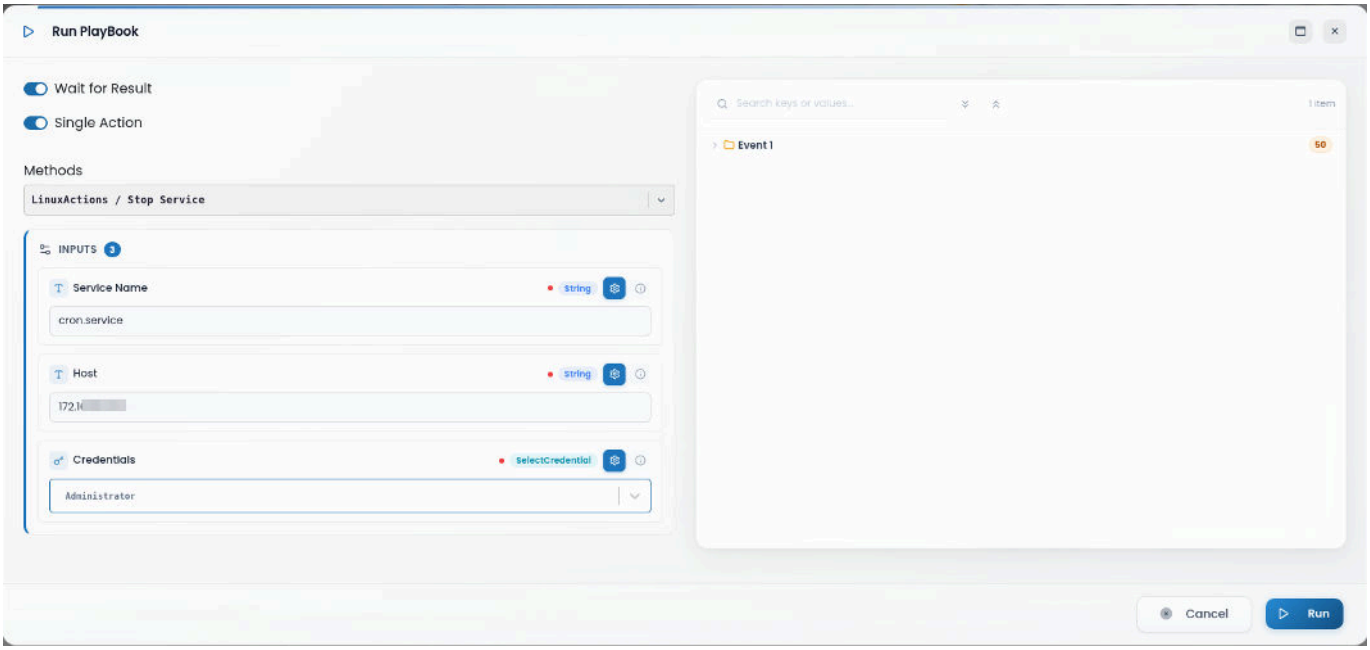
This action is used to start a service.



Inputs	Description
Service Name (is required)	Provide the Service Name
Host (is required)	The target host
Credentials (is required)	The credentials of the Computer that you want to Start a Service

LinuxActions/Stop Service method

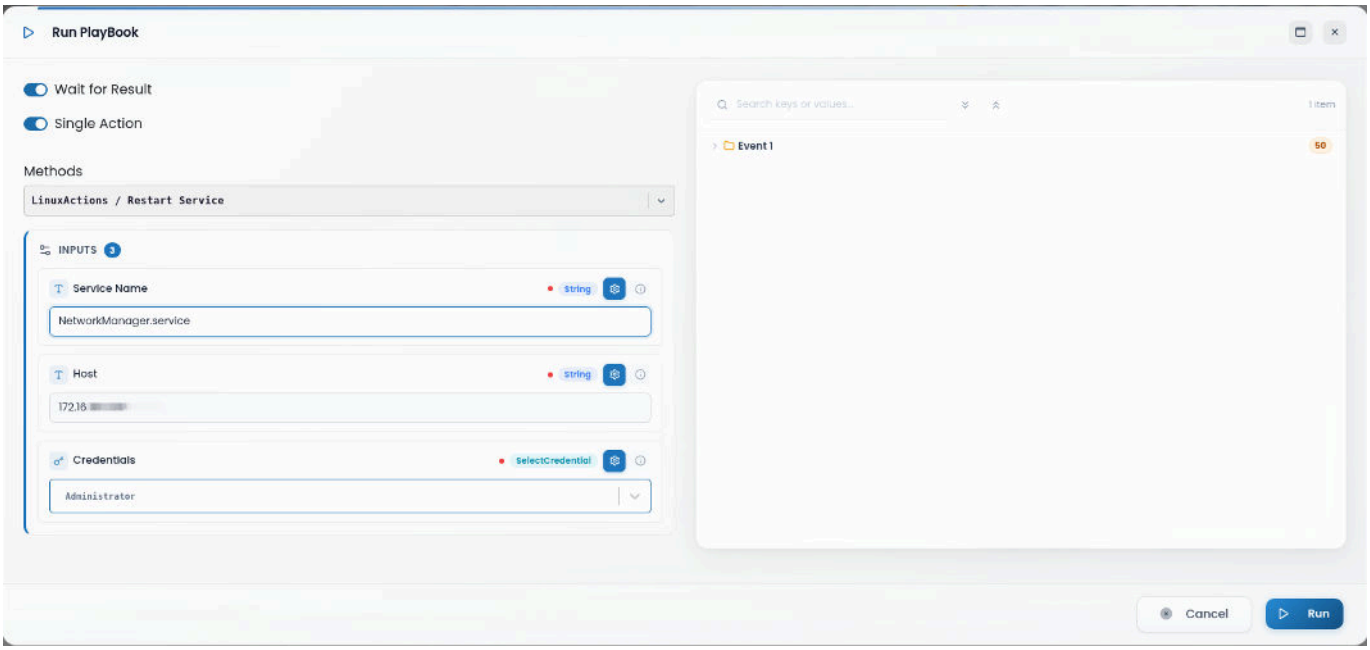
This action is used to stop a service.



Inputs	Description
Service Name (is required)	Provide the Service Name
Host (is required)	The target host
Credentials (is required)	The credentials of the Computer that you want to Stop a Service

LinuxActions/Restart Service method

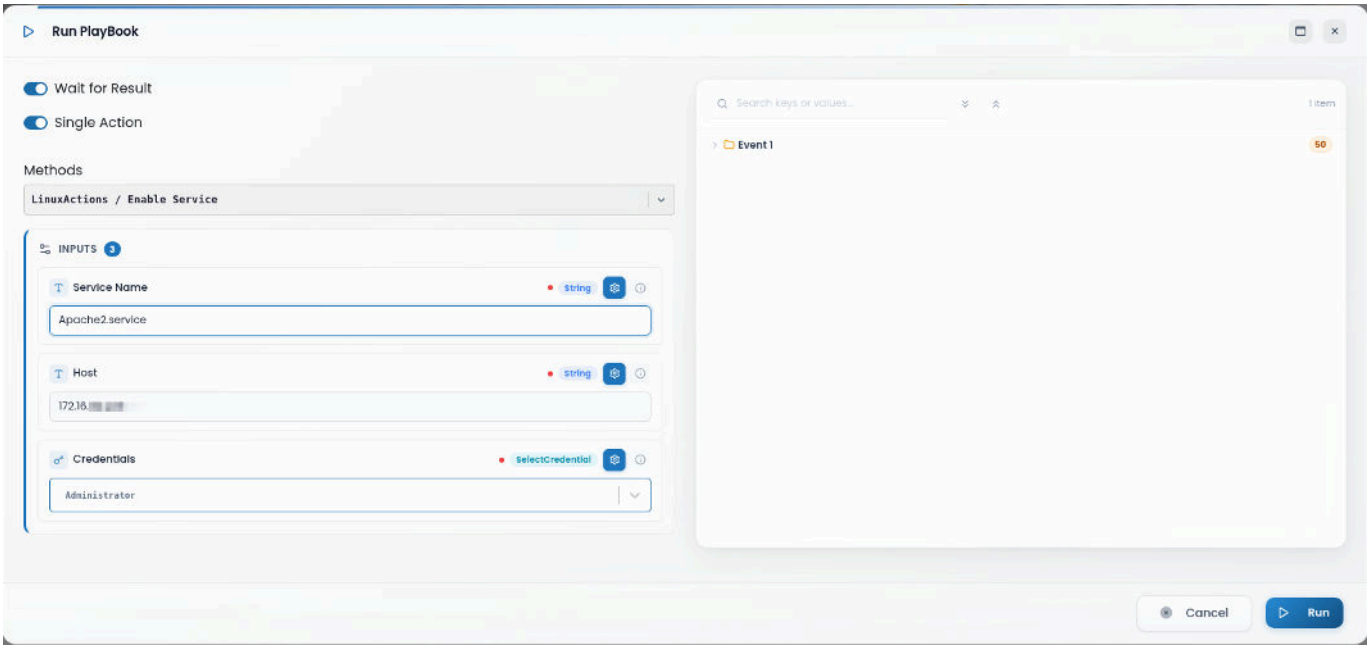
This action is used to restart a service.



Inputs	Description
Service Name (is required)	Provide the Service Name
Host (is required)	The target host
Credentials (is required)	The credentials of the Computer that you want to Restart a Service

LinuxActions/Enable Service method

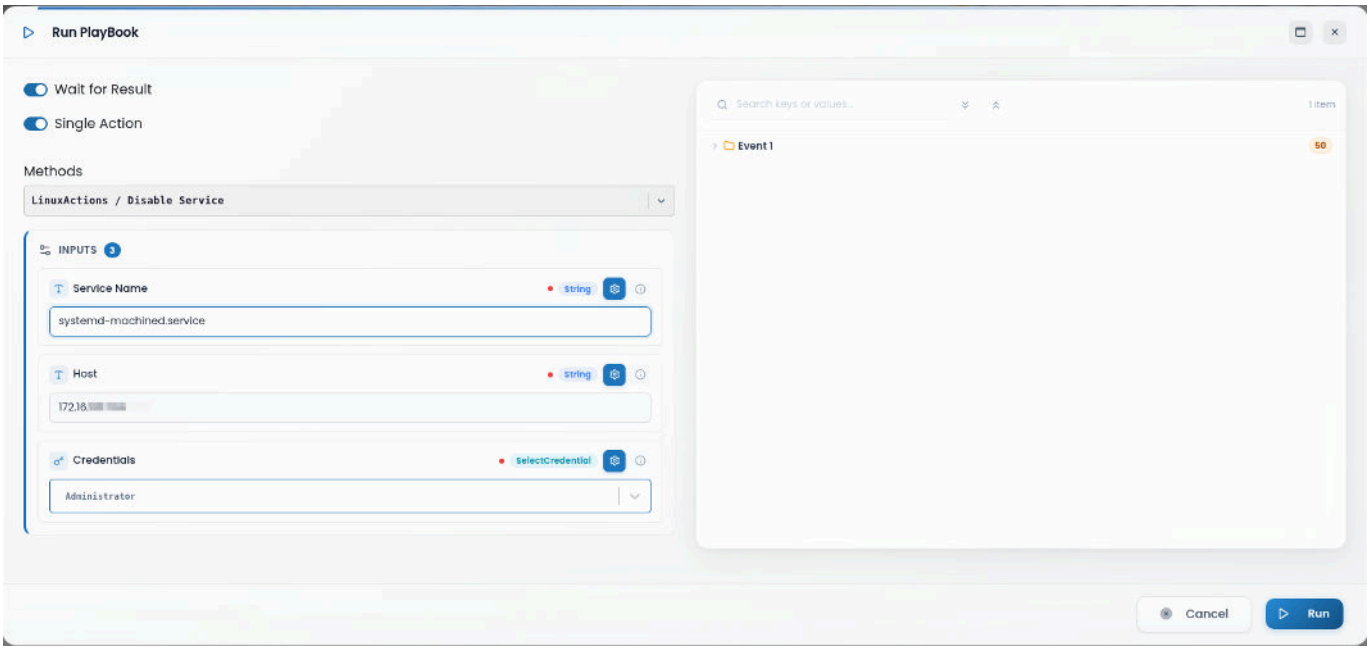
This action is used to enable a service.



Inputs	Description
Service Name (is required)	Provide the Service Name
Host (is required)	The target host
Credentials (is required)	The credentials of the Computer that you want to Enable a Service

LinuxActions/Disable Service method

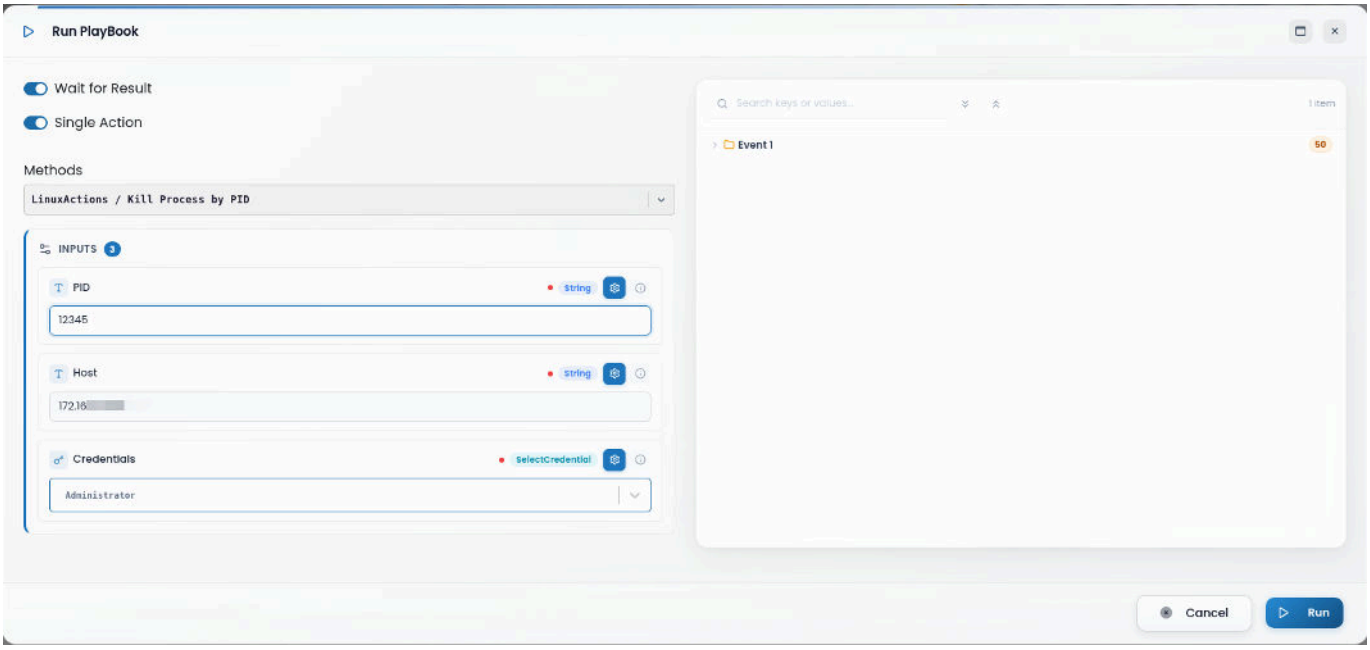
This action is used to enable a service disable a service.



Inputs	Description
Service Name (is required)	Provide the Service Name
Host (is required)	The target host
Credentials (is required)	The credentials of the Computer that you want to Disable a Service

LinuxActions/Kill Process by PID method

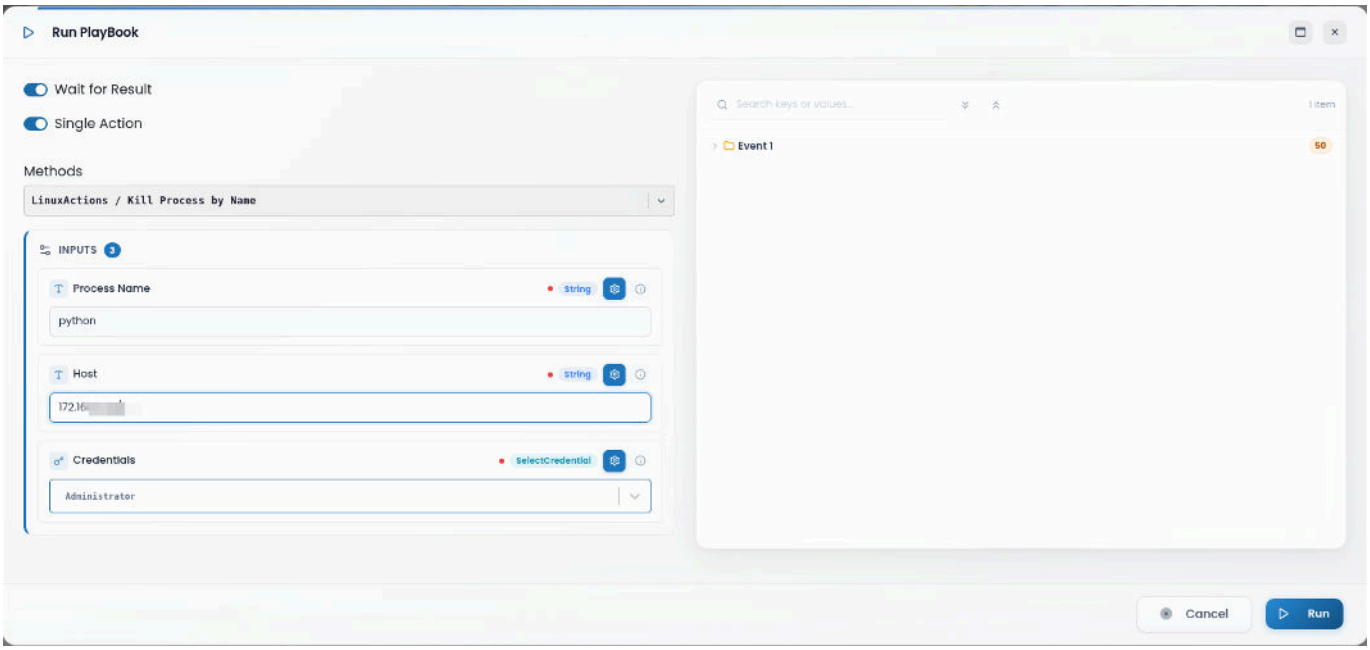
This action is used to Kill a process by PID.



Inputs	Description
PID (is required)	Provide the Process ID (PID)
Host (is required)	The target host
Credentials (is required)	The credentials of the Computer that you want to Kill a Process by Process ID

LinuxActions/Kill Process by Name method

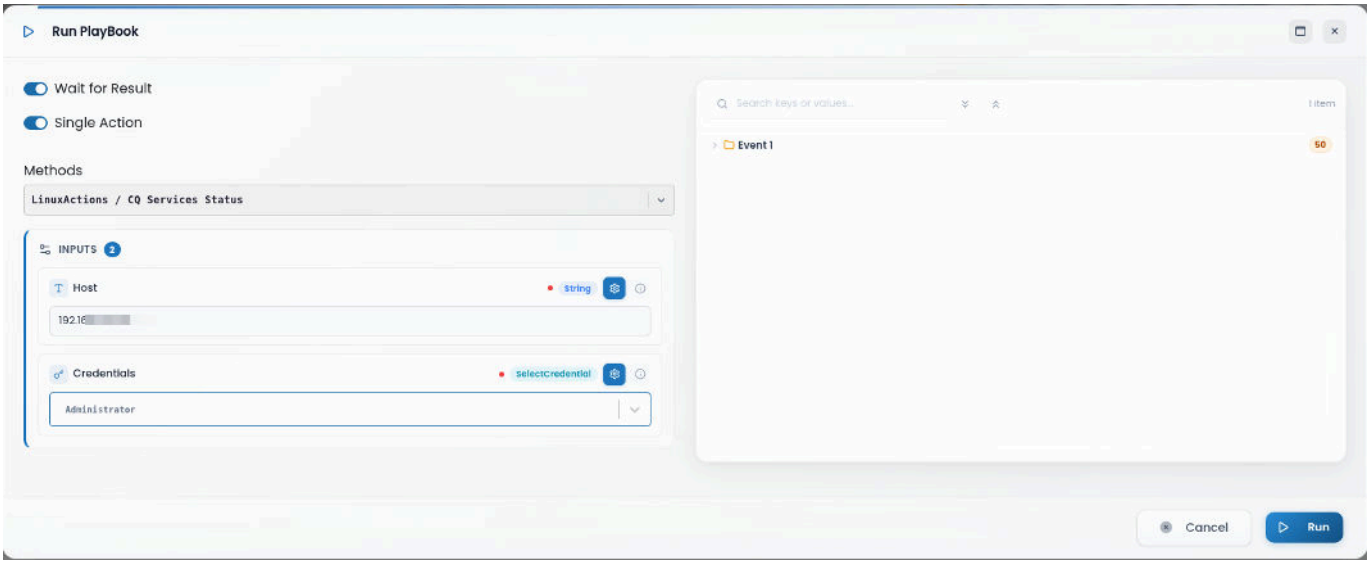
This action is used to Kill a process by name.



Inputs	Description
Process Name (is required)	Provide the Process Name
Host (is required)	The target host
Credentials (is required)	The credentials of the Computer that you want to Kill a Process by Name

LinuxActions/CQ Services Status method

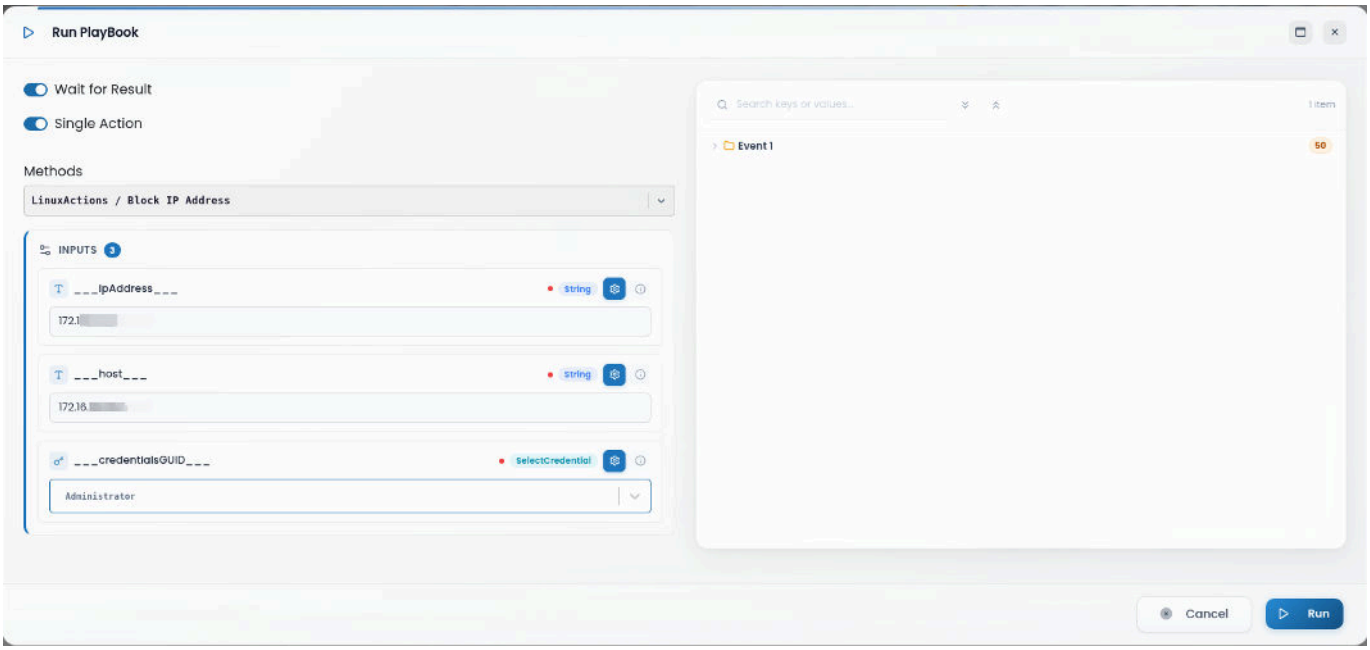
This action is used to check the services status.



Inputs	Description
Host (is required)	The target host
Credentials (is required)	The credentials of the Computer that you want to check the CYBERQUEST Services

LinuxActions/Block IP Address method

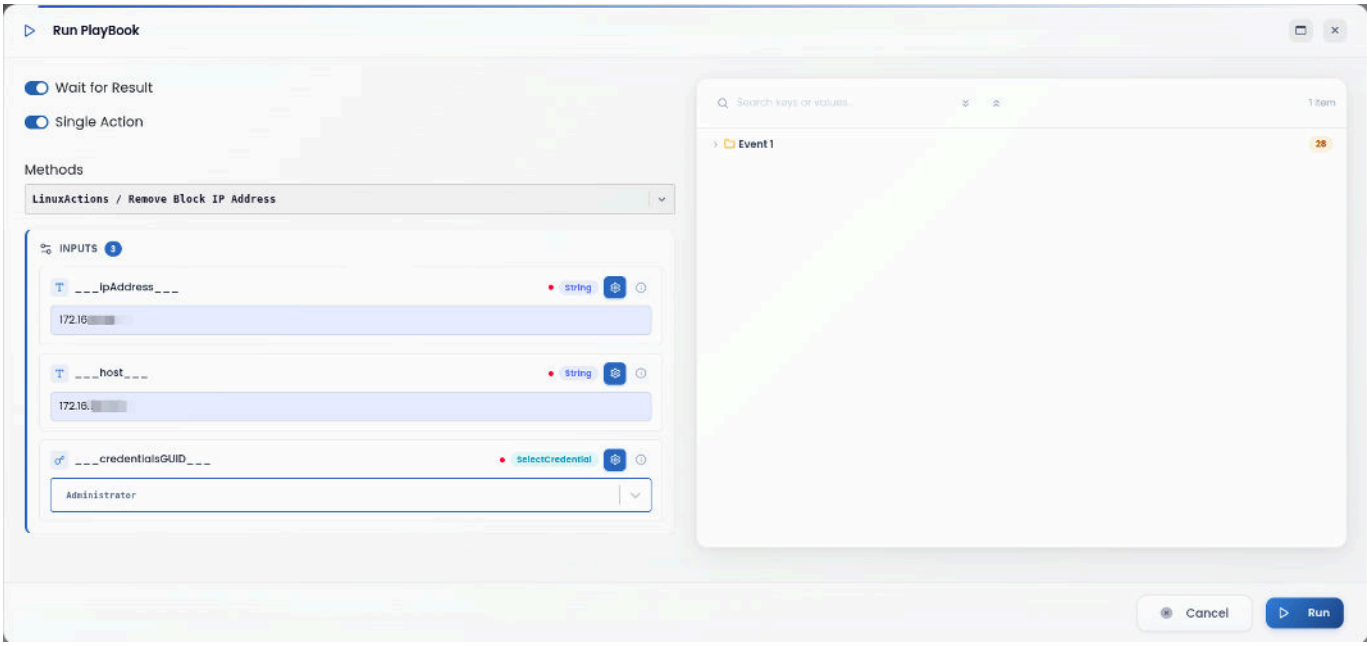
This action is used to Block IP Address.



Inputs	Description
ipAddress (is required)	The IP Address that you want to block
host (is required)	The host that you want to block the IP Address
credentialsGUID (is required)	The credentials of the Computer that you want to block the IP Address

LinuxActions/Remove Block IP Address method

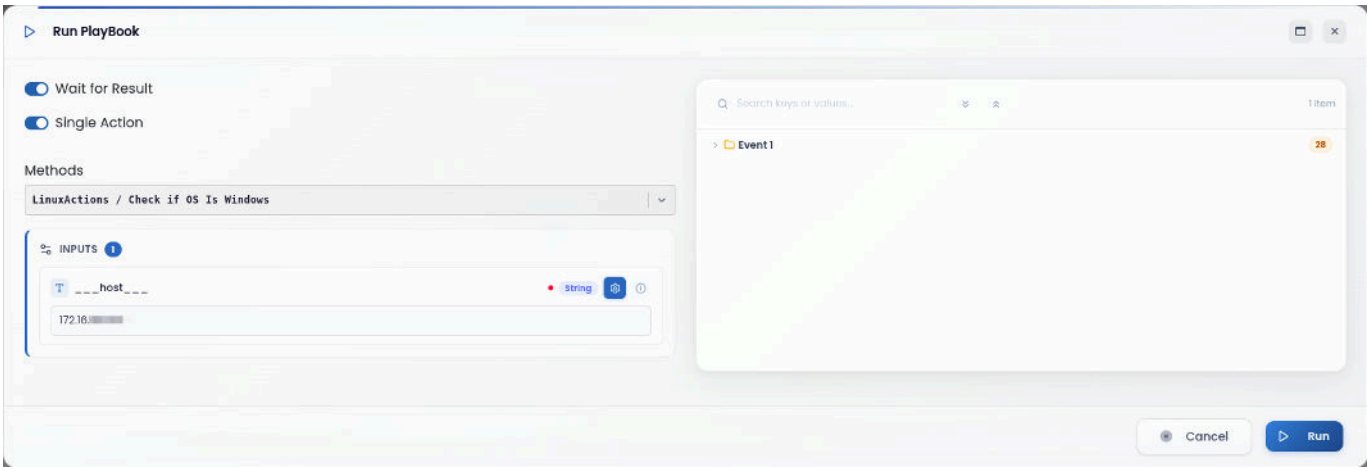
This action is used to Remove Block IP Address.



Inputs	Description
ipAddress (is required)	The blocked IP Address that you want to remove
host (is required)	The host that you want to remove the blocked IP Address
credentialsGUID (is required)	The credentials of the Computer that you want to remove the blocked IP Address

LinuxActions/Check if OS Is Windows method

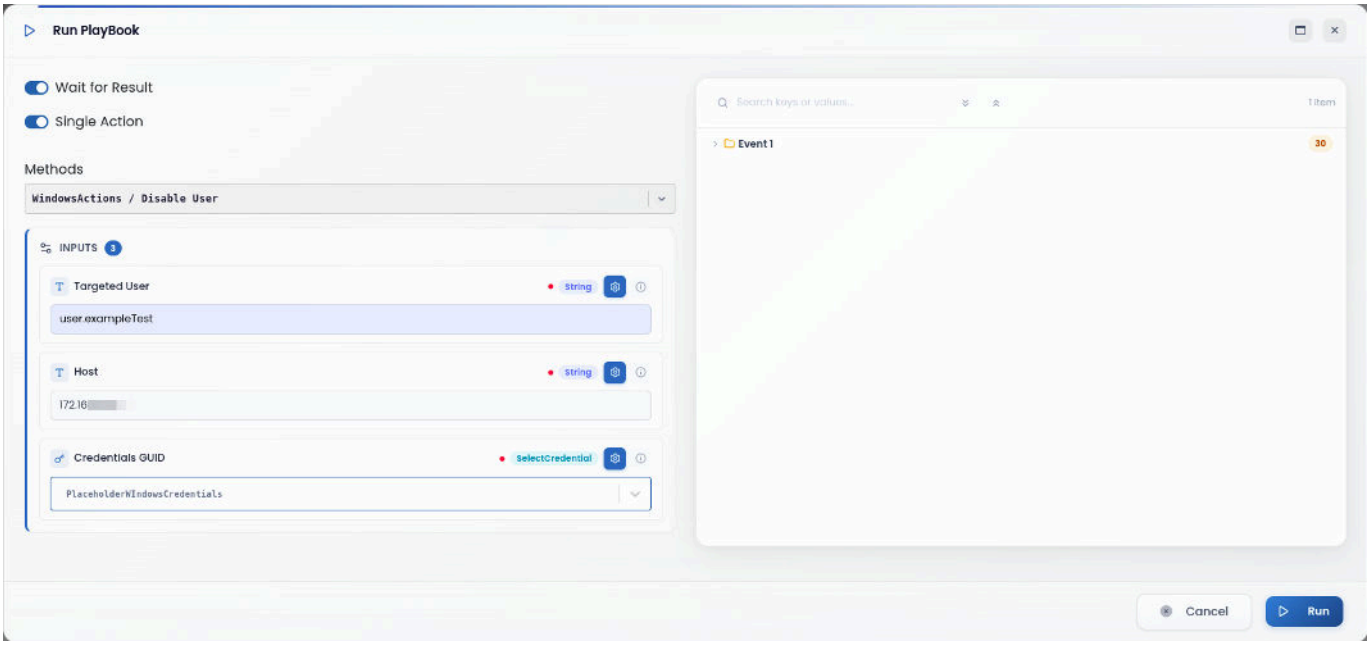
This action is used to check if OS Is Windows.



Inputs	Description
host (is required)	The host that you want to verify the Operating System

WindowsActions/Disable User method

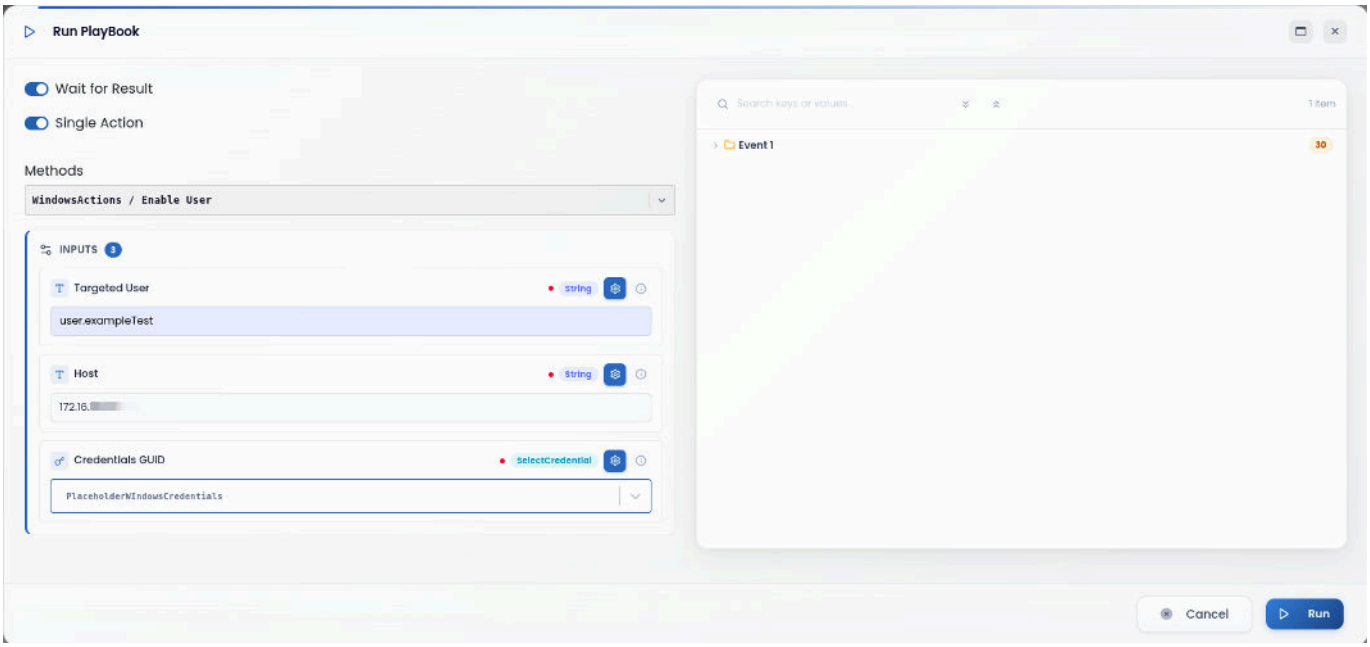
This action is used to disable a User.



Inputs	Description
Targeted User (is required)	The user who is targeted
Host (is required)	The target host
Credentials GUID (is required)	Credentials GUID

WindowsActions/Enable User method

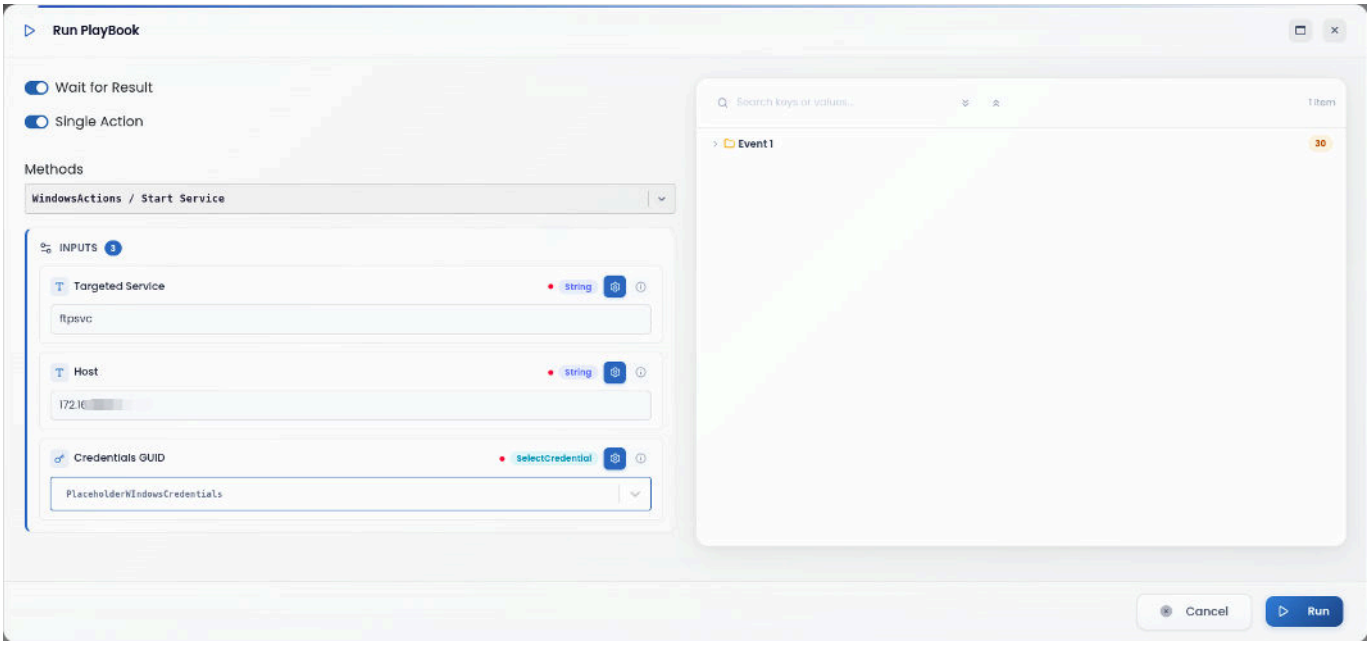
This action is used to enable a User.



Inputs	Description
Target User (is required)	The user who is targeted
Host (is required)	The target host
Credentials GUID (is required)	The credentials of the Computer that you want to disable

WindowsActions/Start Service method

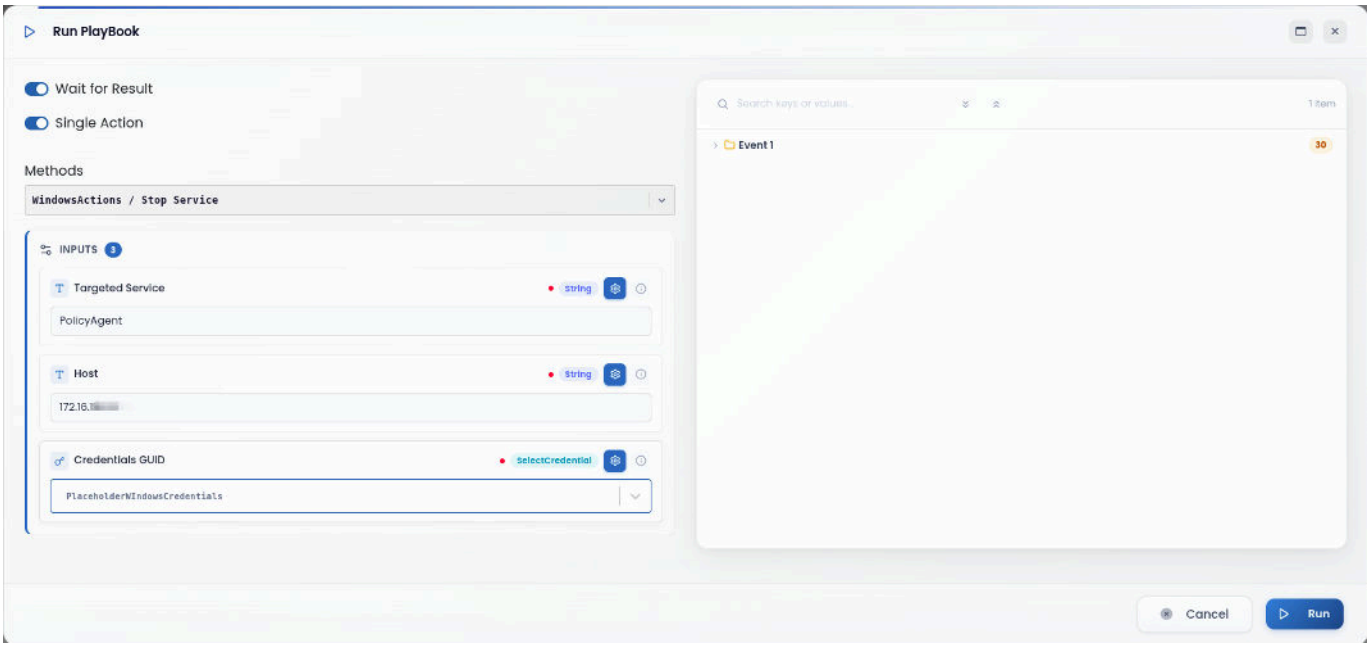
This action is used to start a service.



Inputs	Description
Targeted Service (is required)	Provide the Service Name
Host (is required)	The target host
Credentials GUID (is required)	The credentials of the Computer that you want to Start a Service

WindowsActions/Stop Service method

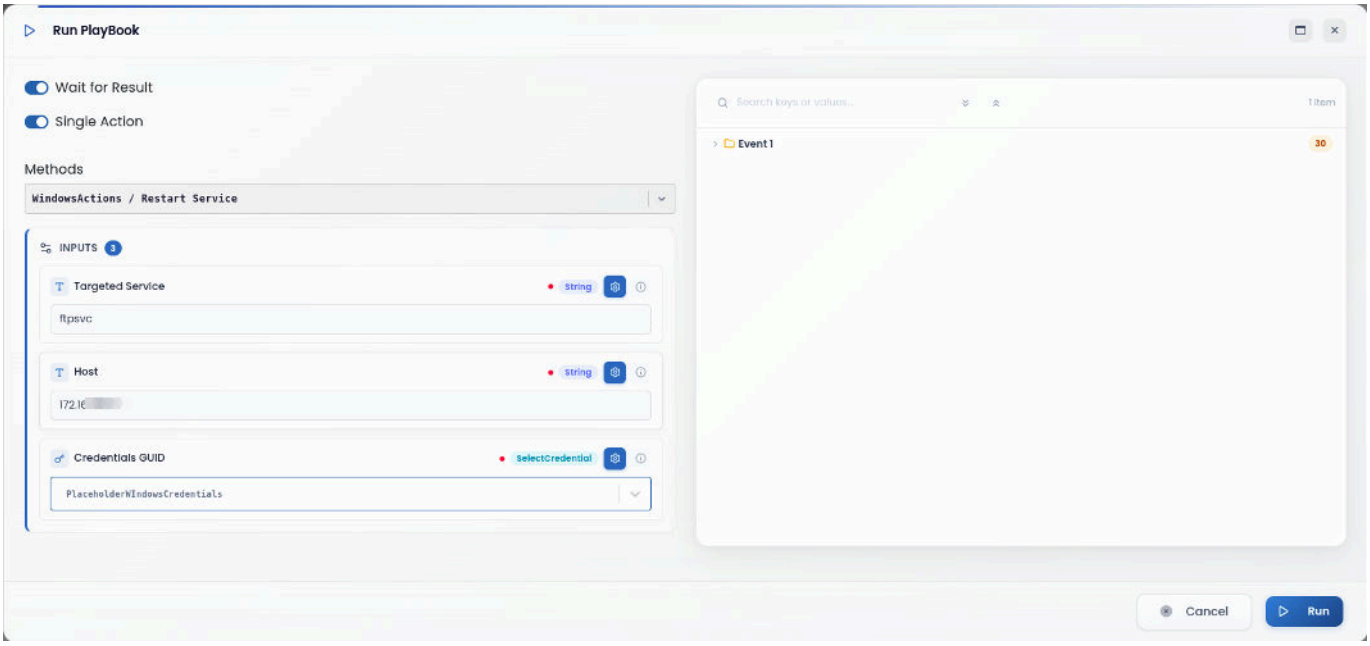
This action is used to stop a service.



Inputs	Description
Targeted Service (is required)	Provide the Service Name
Host (is required)	The target host
Credentials GUID (is required)	The credentials of the Computer that you want to Stop a Service

WindowsActions/Restart Service method

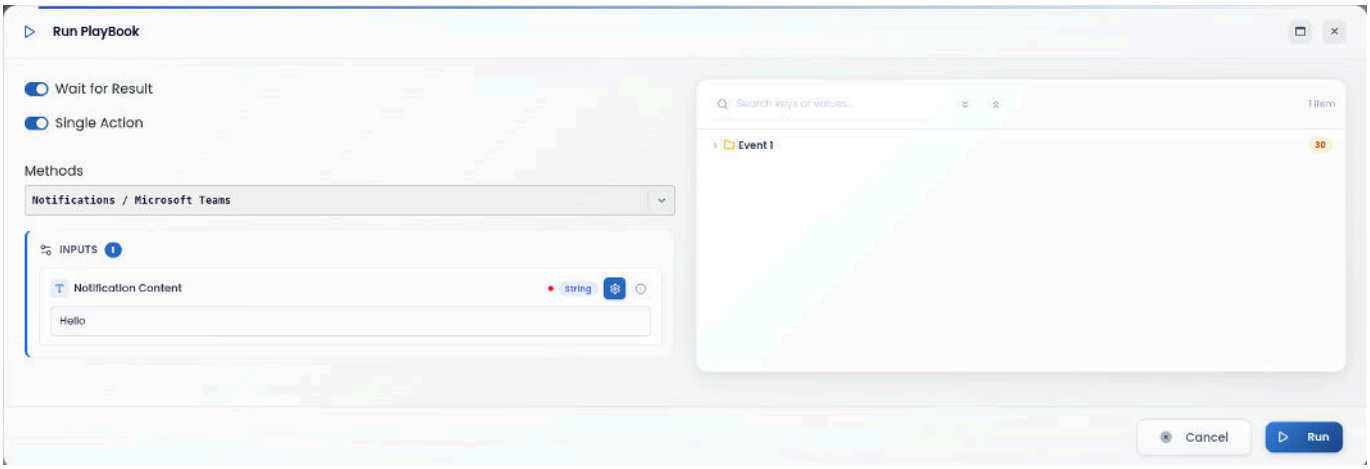
This action is used to restart a service.



Inputs	Description
Targeted Service (is required)	Provide the Service Name
Host (is required)	The target host
Credentials GUID (is required)	The credentials of the Computer that you want to Restart a Service

Notifications/Microsoft Teams method

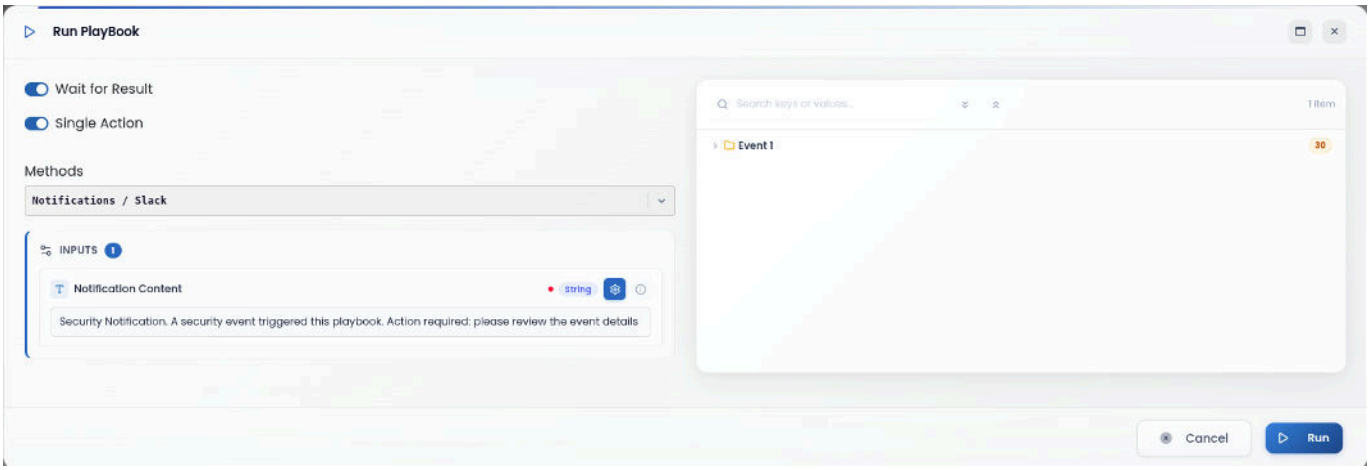
This action help you to send notification to Microsoft Teams.



Inputs	Description
Notification Content (is required)	The content of notification

Notifications/Slack method

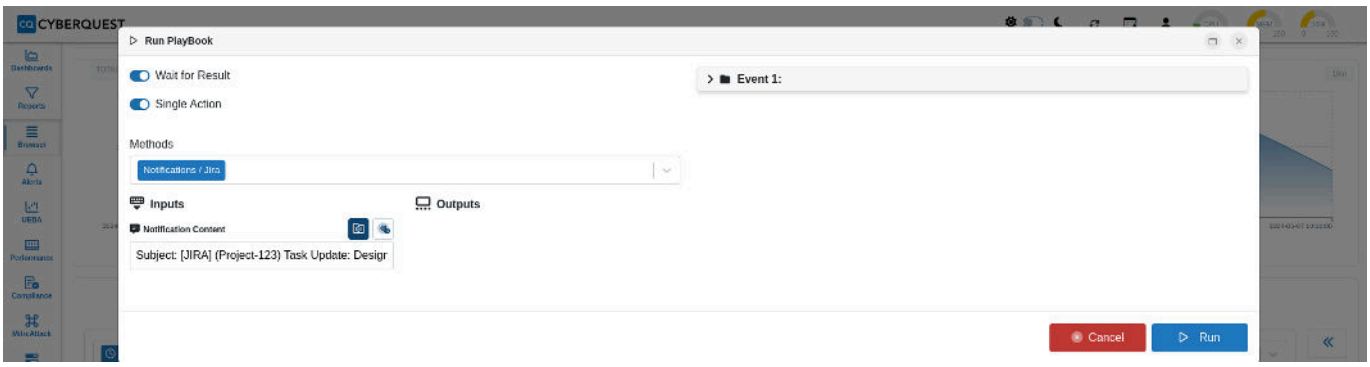
This action help you to send notification to Slack.



Inputs	Description
Notification Content (is required)	The content of notification

Notifications/Jira method

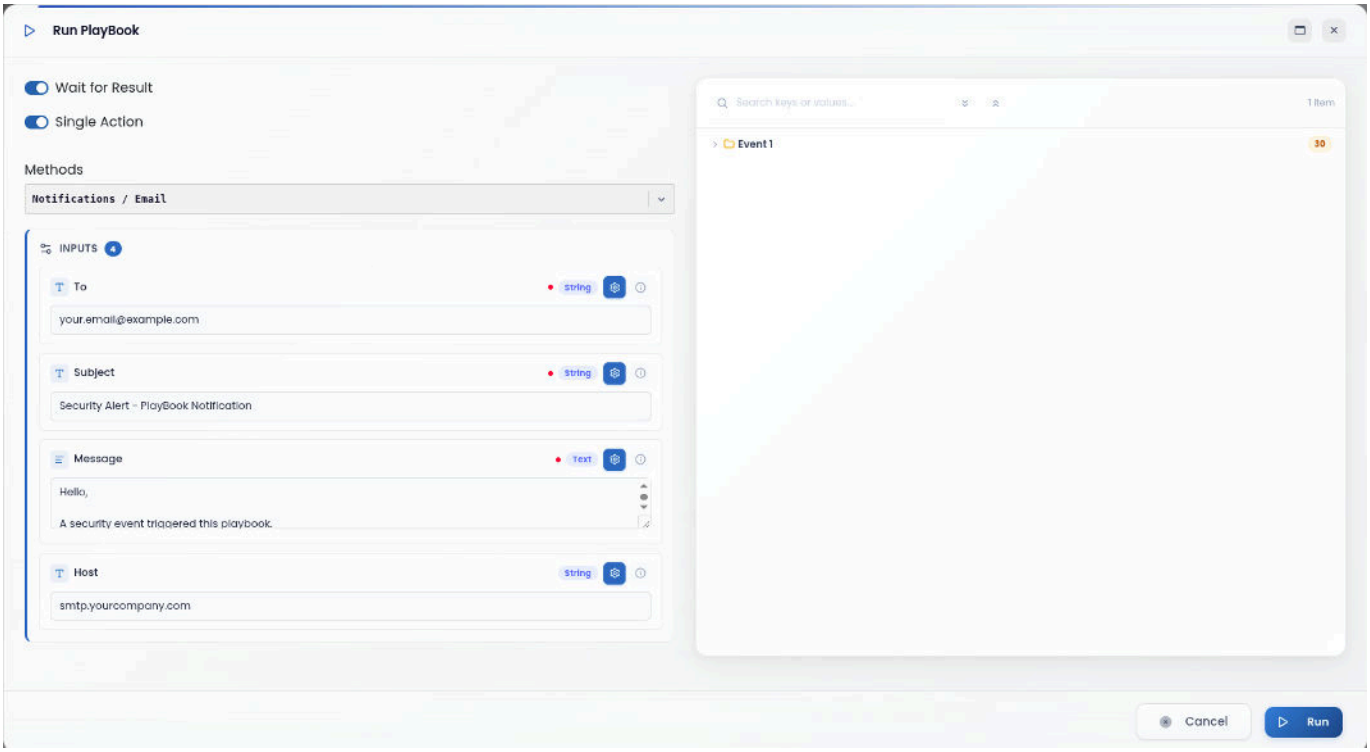
This action help you to send notification to Jira.



Inputs	Description
Notification Content (is required)	The content of notification

Notifications/Email

This action help you to send notification to Email.

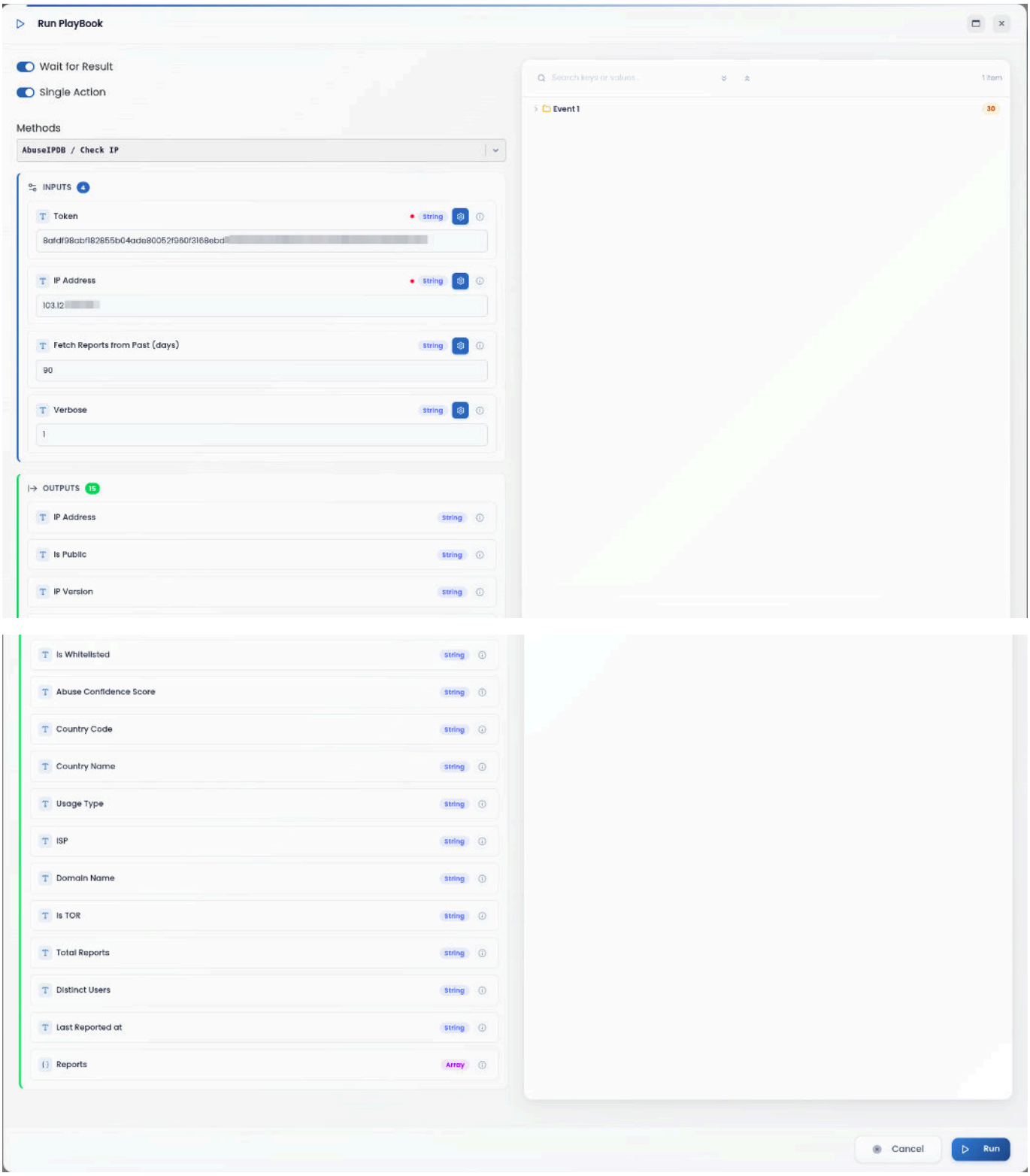


Inputs	Description
To (is required)	To
Subject (is required)	Subject
Message (is required)	Subject

AbuseIPDB

AbuseIPDB/Check IP method

This action executes an AbuseIPDB IP lookup using the IP address you provided.

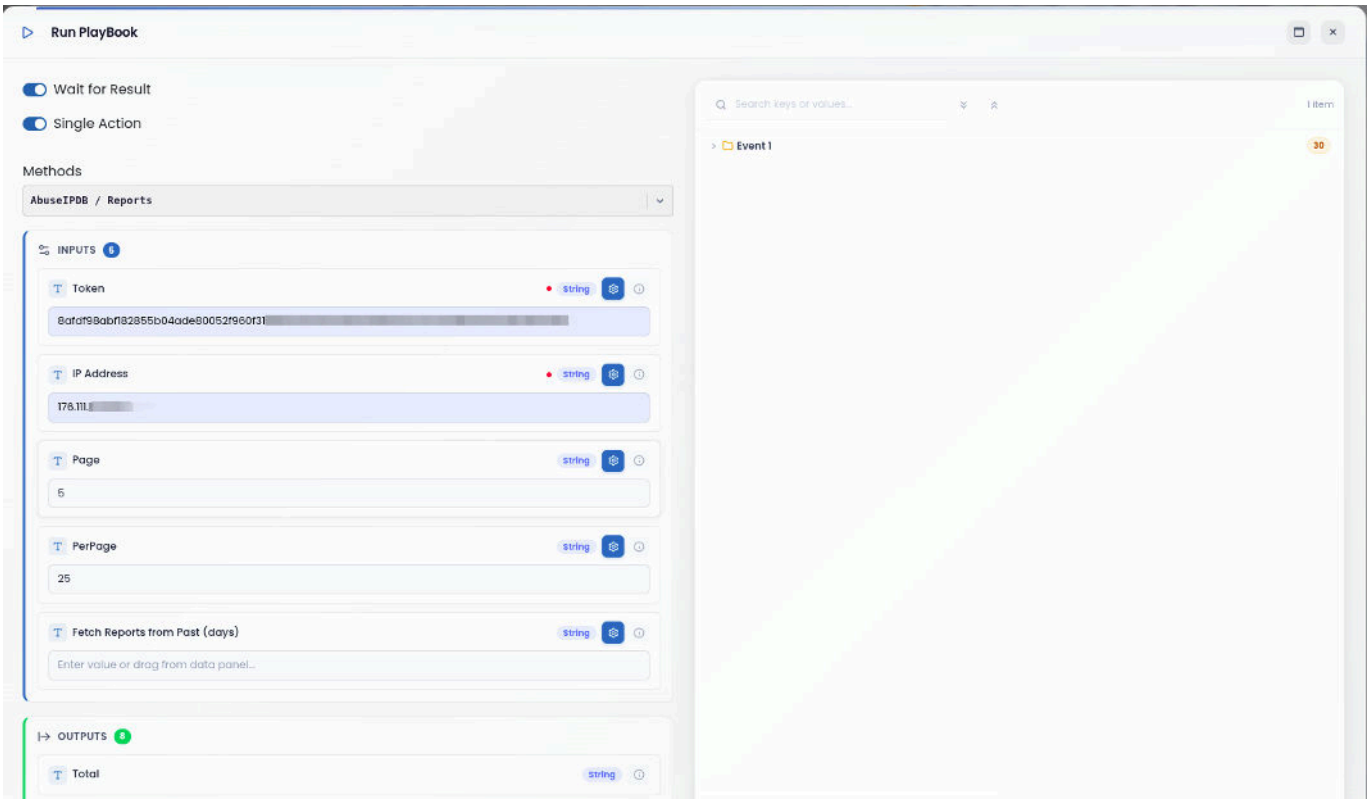


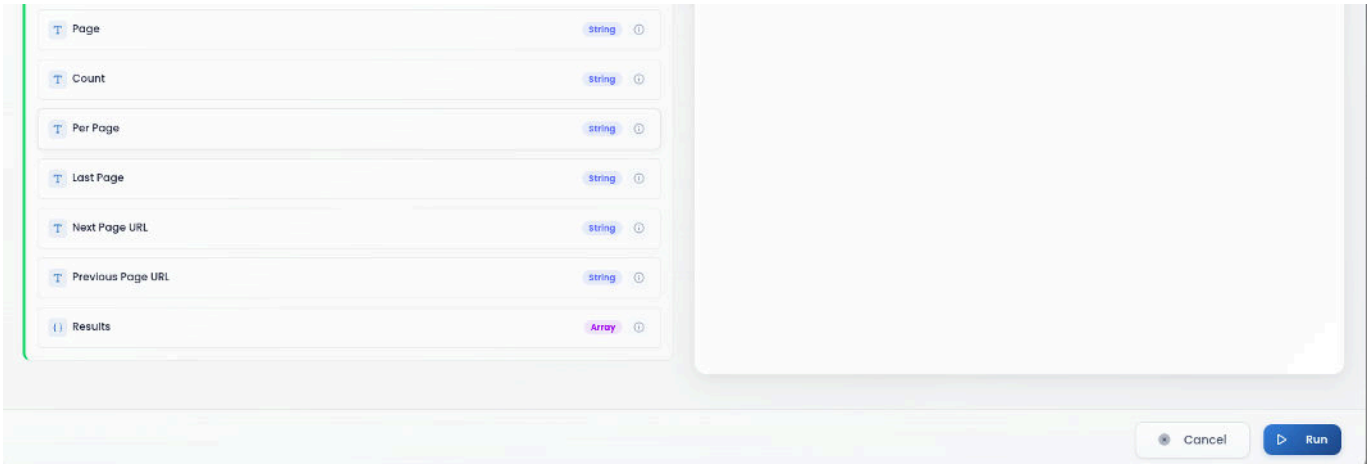
Inputs	Description
Token (is required)	To use the AbuseIPDB API, you must have an API key
IP Address (is required)	The IP Address which is verified by AbuseIPDB
Fetch Reports from Past (days)	The Fetch Reports from Past parameter determines how far back in time(days) we go to fetch reports. By default is 30 days, but not older than 90 days
Verbose	Reports can be included in this response if the verbose flag is added

Outputs	Description
IP Address(ipAddress)	The investigated IP address
Is Public(isPublic)	True or False if the ip is public or not
IP Version(ipVersion)	The version of the investigated IP
Is Whitelisted(isWhitelisted)	True or false if the investigated IP is in Whitelist of AbuseIPDB
Abuse Confidence Score(abuseConfidenceScore)	This score is calculated by AbuseIPDB. This score can be used to take action against a malicious IP
Country Code(countryCode)	The country code from which the investigated IP originates
Country Name(countryName)	The country name from which the investigated IP originates
Usage Type(usageType)	The general use of the investigate IP address (for example: Comercial, Organization, Government, Military, etc.)
ISP(isp)	The name of the Internet Service Provider which provided the IP which is investigated
Domain Name(domain)	The domain name of the ISP which provided the IP which is investigated
Is TOR(isTor)	True or False if the investigated IP was seen in TOR nodes
Total Reports(totalReports)	The total number of registered reports about the investigated IP
Distinct Users(numDistinctUsers)	The number of distinct users who reported the investigated IP
Last Reported at(lastReportedAt)	The date when the investigated IP was last time reported
Reports(reports)	The list of reports for the investigated IP

AbuseIPDB/Reports method

This action get reports about IP address.



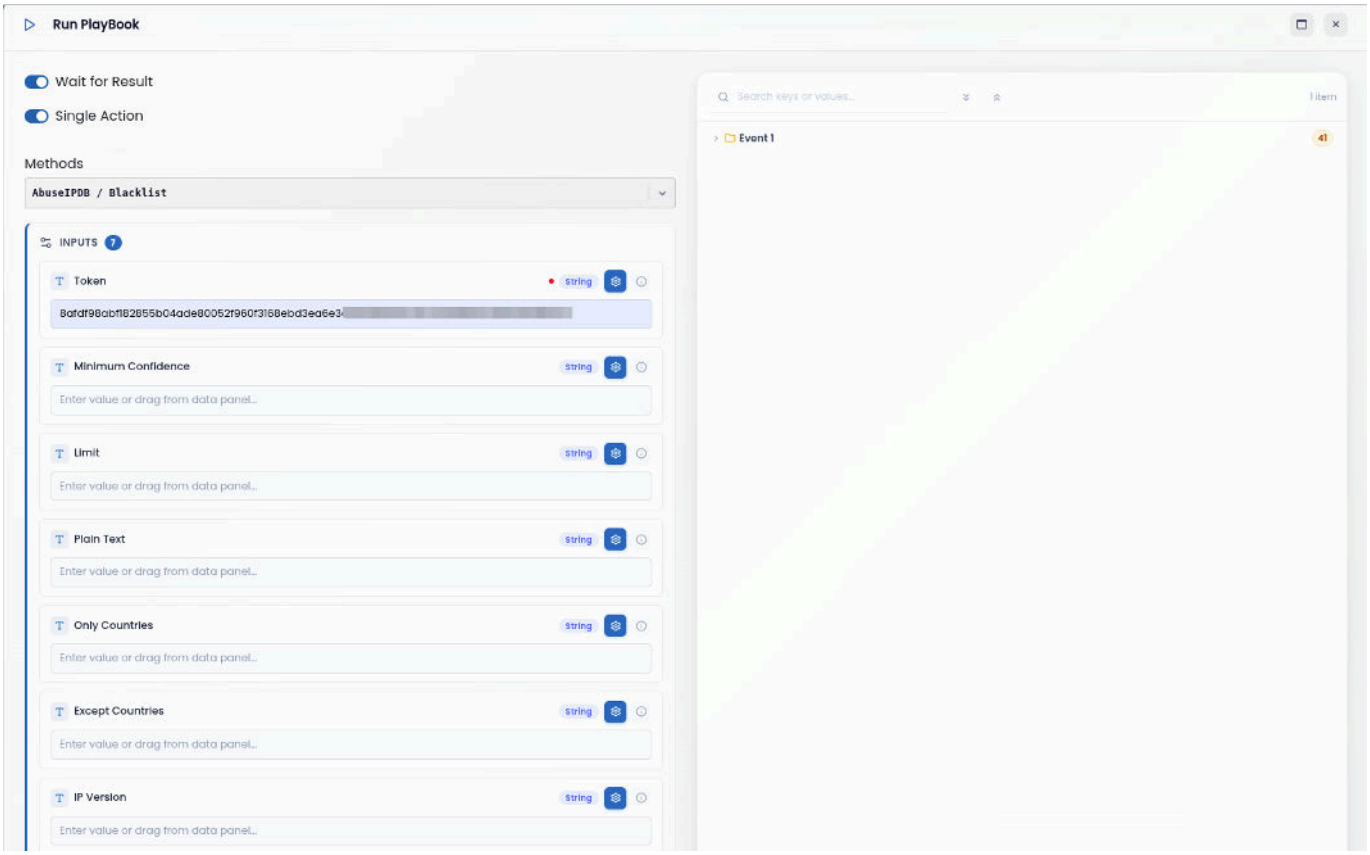


Inputs	Description
Token (is required)	To use the AbuseIPDB API, you must have an API key
IP Address (is required)	The IP address which is verified
Page	Navigate the created pagination via PerPage parameter
PerPage	Adjust the pagination
Fetch Reports from Past (days)	The Fetch Reports from Past parameter determines how far back in time(days) we go to fetch reports. By default is 30 days, but not older than 90 days

Outputs	Description
Total(total)	Total number of reports for investigated IP
Page(page)	The page number of reports list
Count(count)	The number of reports presented in the page
Per Page(perPage)	How many reports are listed by page
Last Page(lastPage)	The number of the last page which contains reports
Next Page URL(nextPageUrl)	The URL of the next page which contains reports
Previous Page URL(previousPageUrl)	The URL of the previous page which contains reports
Results(results)	The reports listed by page

AbuseIPDB/Blacklist method

This action depending on the input settings you have chosen, AbuseIPDB will return a list of all reported IP addresses or a list of a specific subset of reported IP addresses.

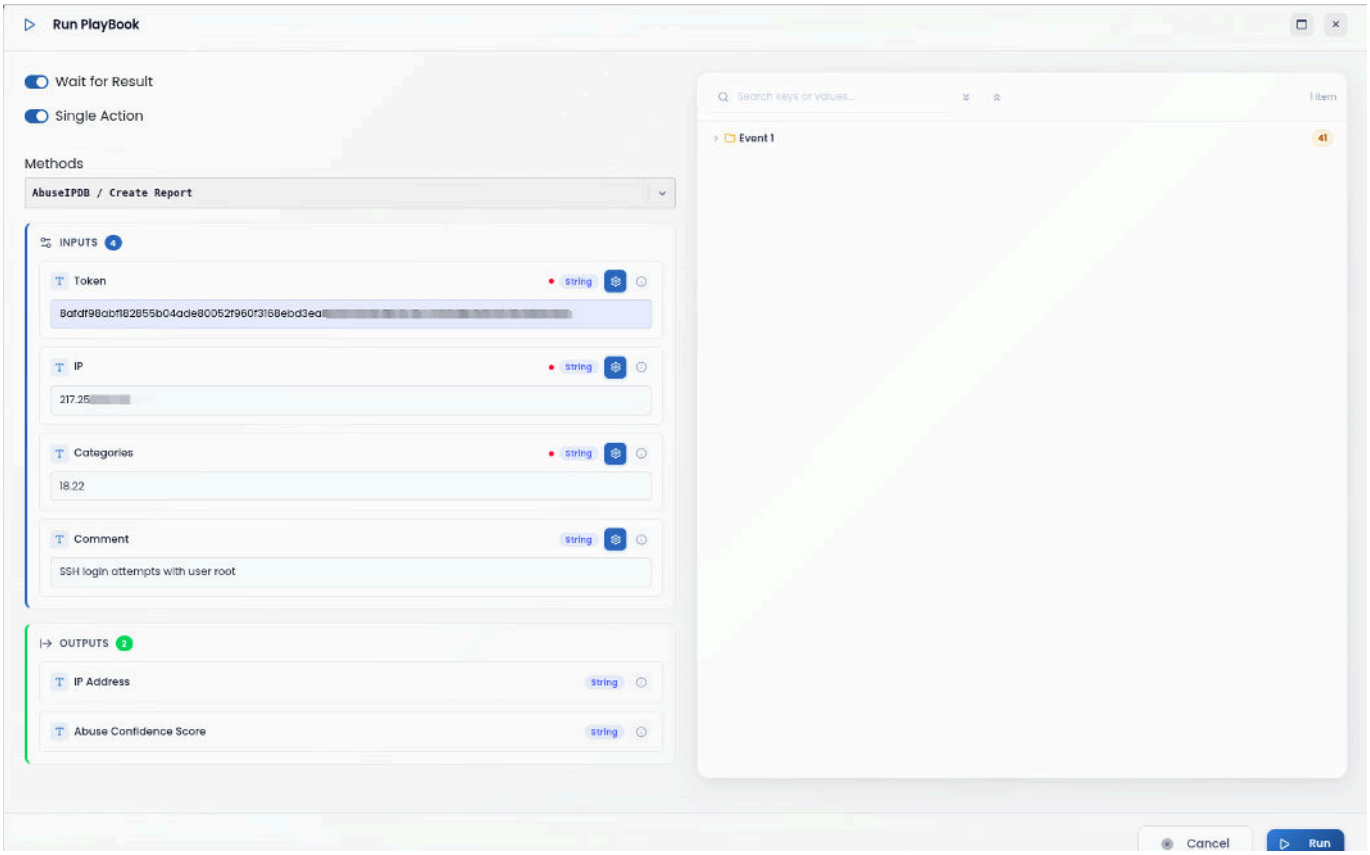


Inputs	Description
Token (is required)	To use the AbuseIPDB API, you must have an API key
Minimum Confidence	It helps to determine the level of trust or reliability assigned to the reported information associated with an IP address
Limit	The number of IP addresses included in the list
Plain Text	Set the Plain Text flag if you prefer a simple newline-separated plaintext response
Only Countries	This parameter retrieves IPs that only originate in the given country or countries
Except Countries	This parameter retrieves all IPs except those that originate in the given country or countries
IP Version	Filter results by IP version (v4 or v6) with this parameter

Outputs	Description
Generated at(generatedAt)	The date when the blacklist was generated
Data(data)	List of blacklisted IPs and additional details (Abuse Confidence Score and date the IP was last reported)

AbuseIPDB/Create Report method

Based on the IP address and malware category you have chosen, reports a specific IP address that has been linked to malicious online activity to AbuseIPDB.

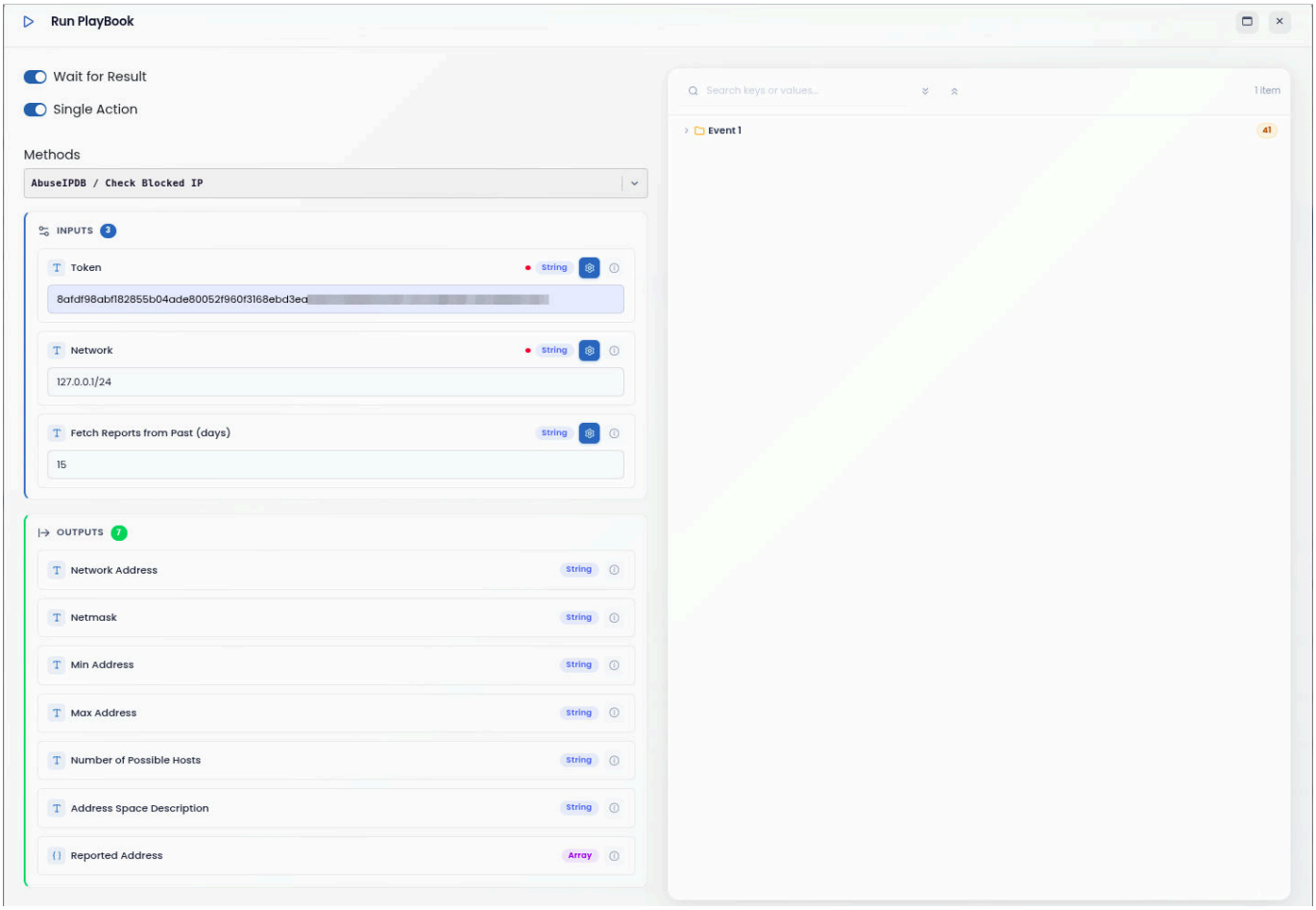


Inputs	Description
Token (is required)	To use the AbuseIPDB API, you must have an API key
IP (is required)	The reported IP address (IPv4 or IPv6)
Categories (is required)	The category in which the IP will be reported
Comment	Related information (server logs, timestamps, etc.)

Outputs	Description
IP Address(ipAddress)	The reported IP Address
Abuse Confidence Score(abuseConfidenceScore)	This score is calculated by AbuseIPDB. This score can be used to take action against a malicious IP

AbuseIPDB/Check Blocked IP method

This action check if the IP is block.

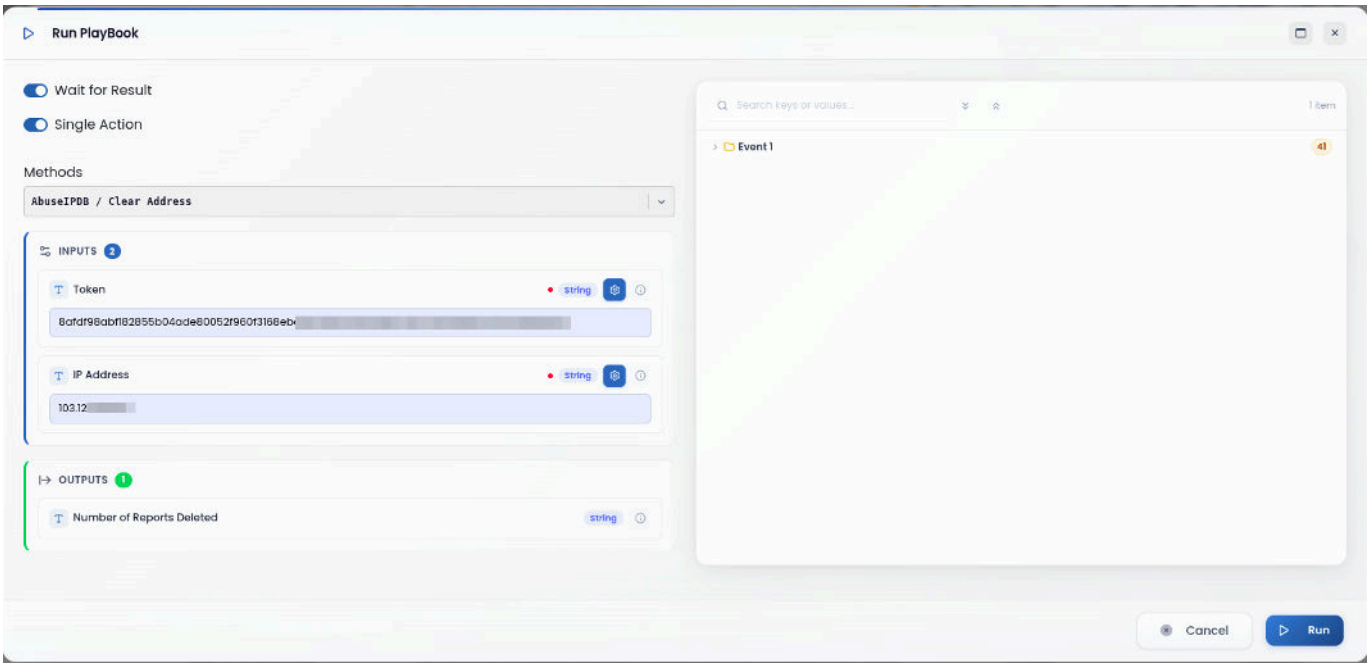


Inputs	Description
Token (is required)	To use the AbuseIPDB API, you must have an API key
Network (is required)	The network address that will be queried
Fetch Reports from Past (days)	The Fetch Reports from Past parameter determines how far back in time(days) we go to fetch reports. By default is 30 days, but not older than 90 days

Outputs	Description
Network Address(networkAddress)	The starting IP address of the subnet
Netmask(netmask)	The subnet mask
Min Address(minAddress)	The minimum IP address within the subnet
Max Address(maxAddress)	The maximum IP address within the subnet
Number of Possible Hosts(numPossibleHosts)	The total number of possible hosts in the subnet
Address Space Description(addressSpaceDesc)	A description of the address space (e.g., “Loopback”)
Reported Address(reportedAddress)	For each IP address within the subnet, the following details are provided: **ipAddress**: The specific IP address; **numReports**: The total number of abuse reports for that IP; **mostRecentReport**: The timestamp of the most recent report; **abuseConfidenceScore**: A calculated evaluation of how abusive the IP is based on user reports; **countryCode**: The country code (if available).

AbuseIPDB/Clear Address method

This action clear an IP address.



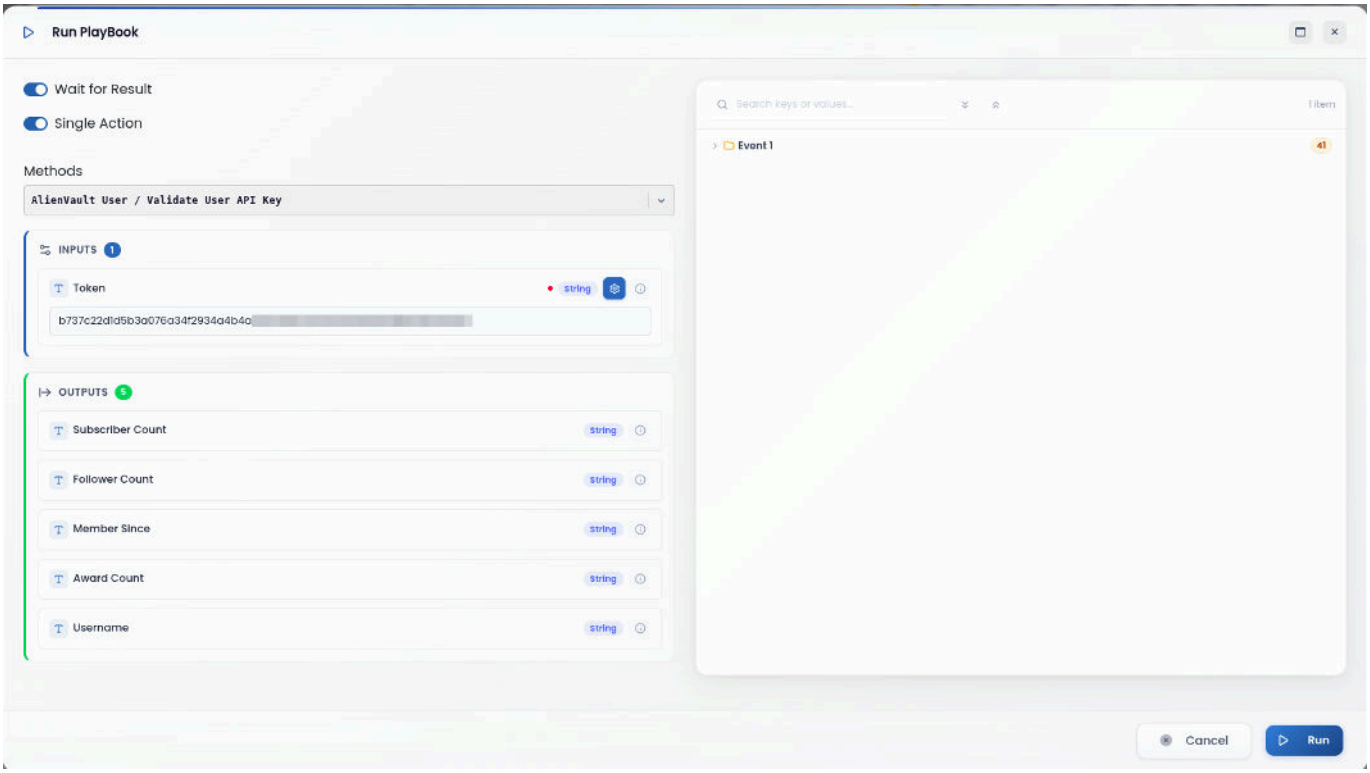
Inputs	Description
Token (is required)	To use the AbuseIPDB API, you must have an API key
IP Address (is required)	The IP address which is cleared
Fetch Reports from Past (days)	The Fetch Reports from Past parameter determines how far back in time(days) we go to fetch reports. By default is 30 days, but not older than 90 days

Outputs	Description
Number of Reports Deleted(numReportsDeleted)	The number of reports deleted associated with the specified IP address reported by you (you cant delete reports from another user account)

AlienVault

AlienVault User/Validate User API Key method

Validate your API Key configuration.

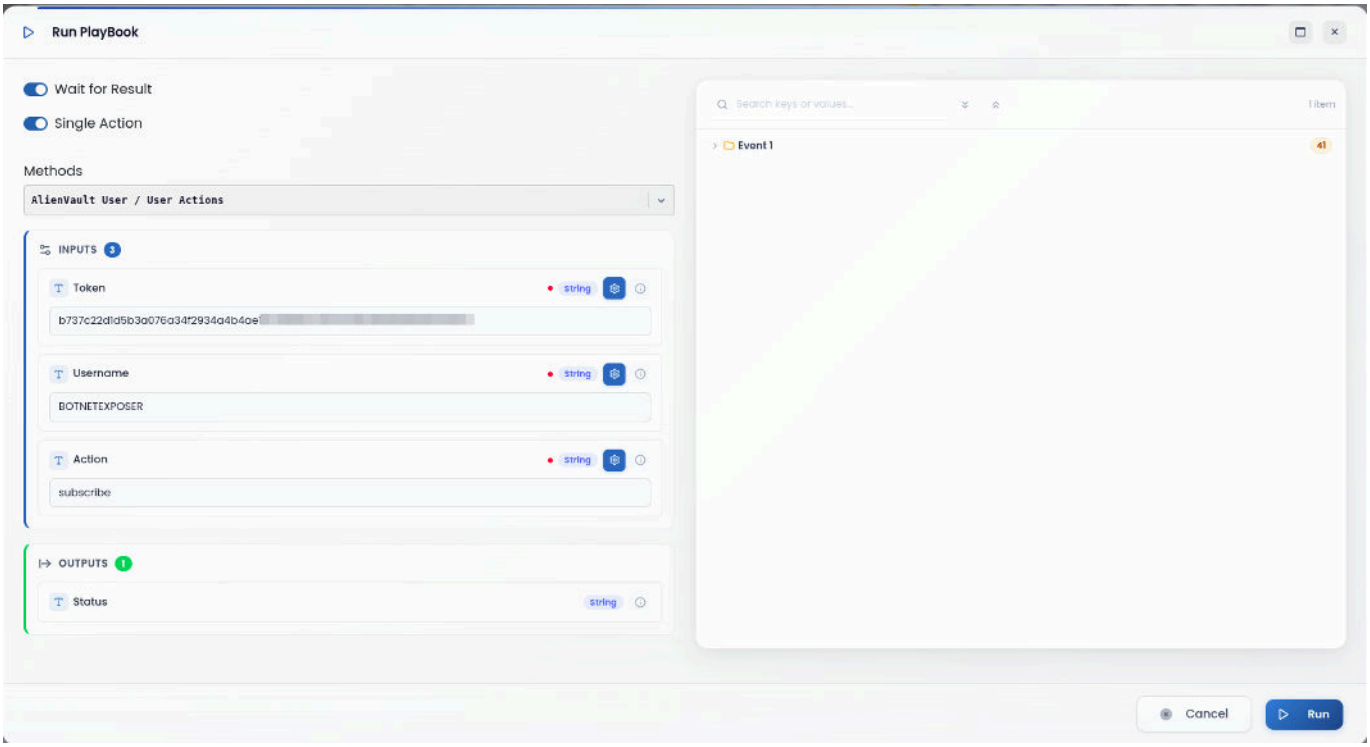


Inputs	Description
Token (is required)	To use the AlienVault API, you must have an API key

Outputs	Description
Subscriber Count(subscriber_count)	The number of subscribers of the user
Follower Count(follower_count)	The number of followers of the user
Member Since(member_since)	The timestamp of the creation of the account of the user
Award Count(award_count)	The number of awards of the user
Username(username)	The username of the user

AlienVault User/User Actions method

Perform actions like follow/subscribe to other users by username.

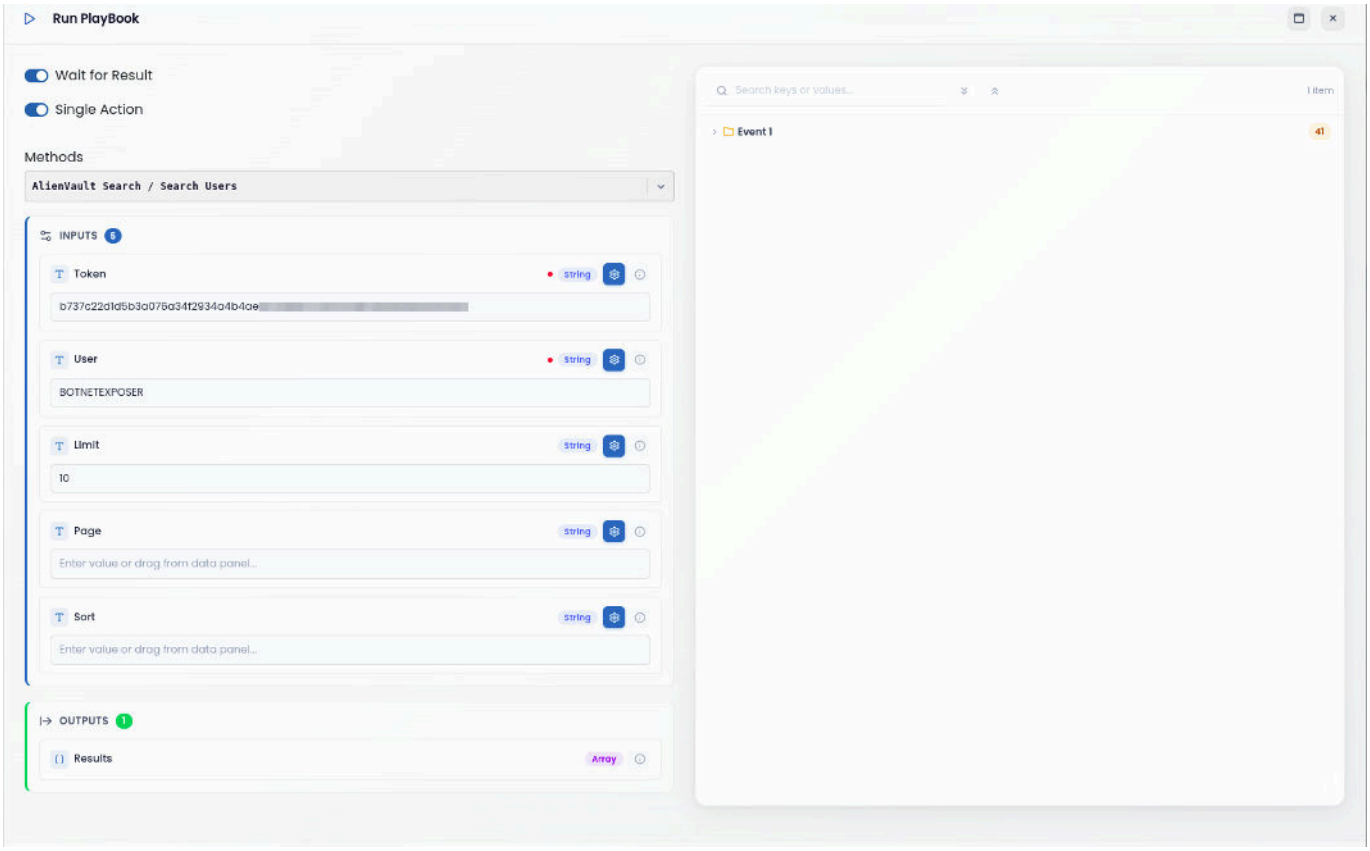


Inputs	Description
Token (is required)	To use the AlienVault API, you must have an API key
Username (is required)	The user on whom the action takes place
Action (is required)	The action that will happen: subscribe, unsubscribe, follow, unfollow

Outputs	Description
Status(status)	The status of API call

AlienVault Search/Search Users method

Search for users matcing query.

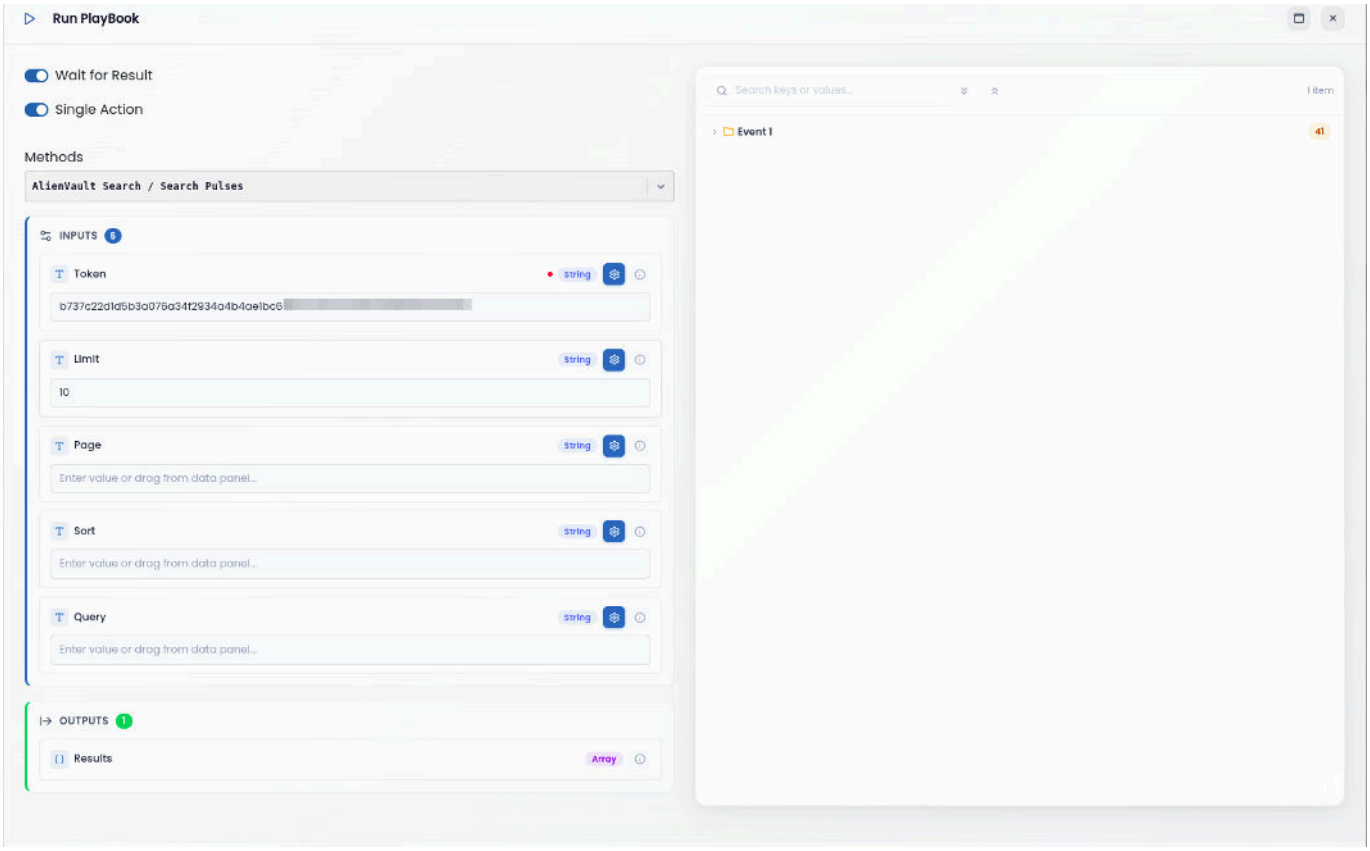


Inputs	Description
Token (is required)	To use the AlienVault API, you must have an API key
User (is required)	Query string to search results with
Limit	Number of results to include per page
Page	Which page of results is desired
Sort	Order by one of these fields: username, pulse_count

Outputs	Description
Results(results)	The results of the API call

AlienVault Search/Search Pulses method

Search for pulses matcing query.

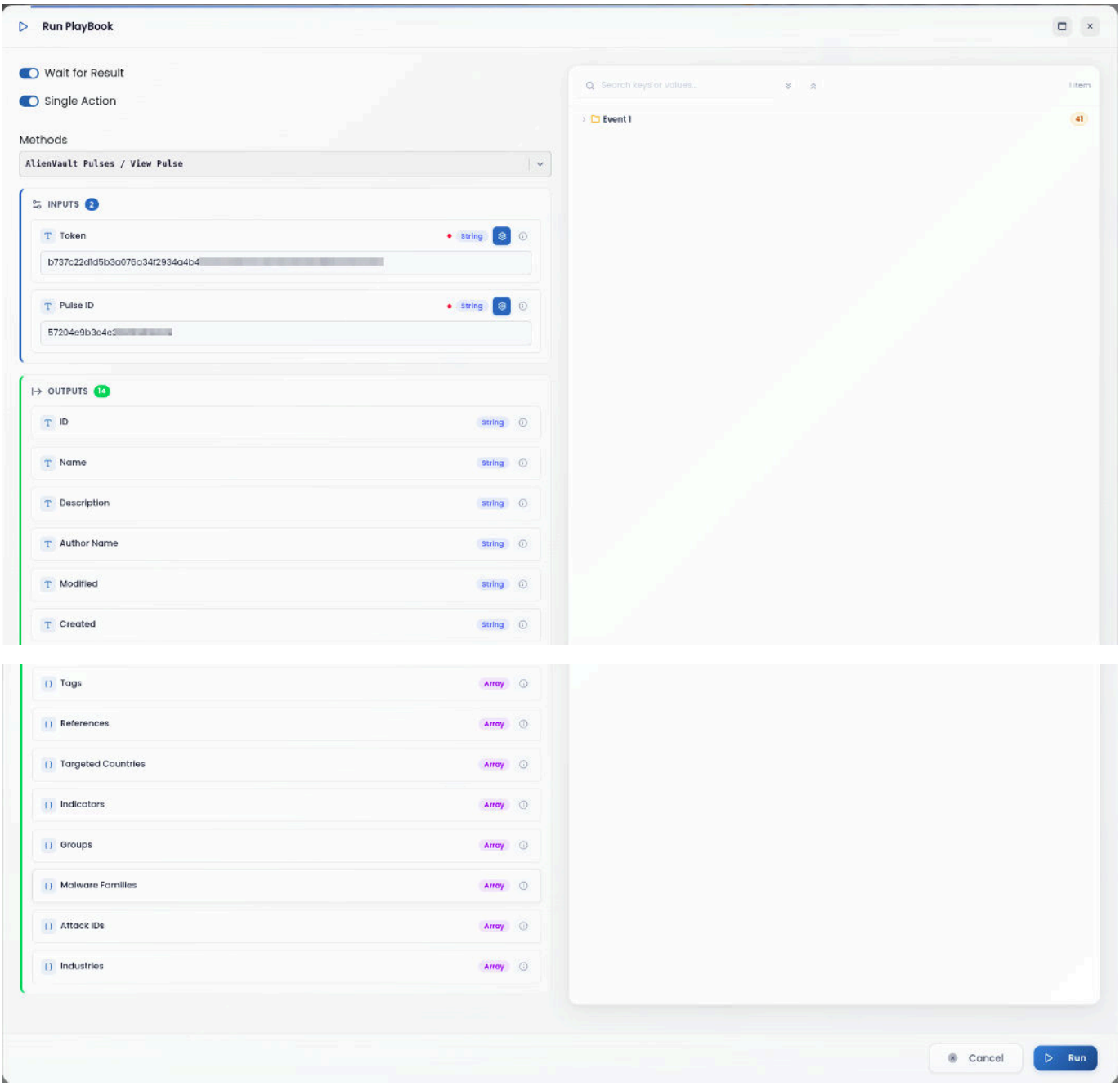


Inputs	Description
Token (is required)	To use the AlienVault API, you must have an API key
Limit	Number of results to include per page
Page	Which page of results is desired
Sort	Order by one of these fields: modified, created, subscriber_count
Query	Query string to search results with

Outputs	Description
Results(results)	The results of the API call

AlienVault Pulses/View Pulse method

View or edit of pulse with id pulse_id. When editing a pulse, use PATCH.

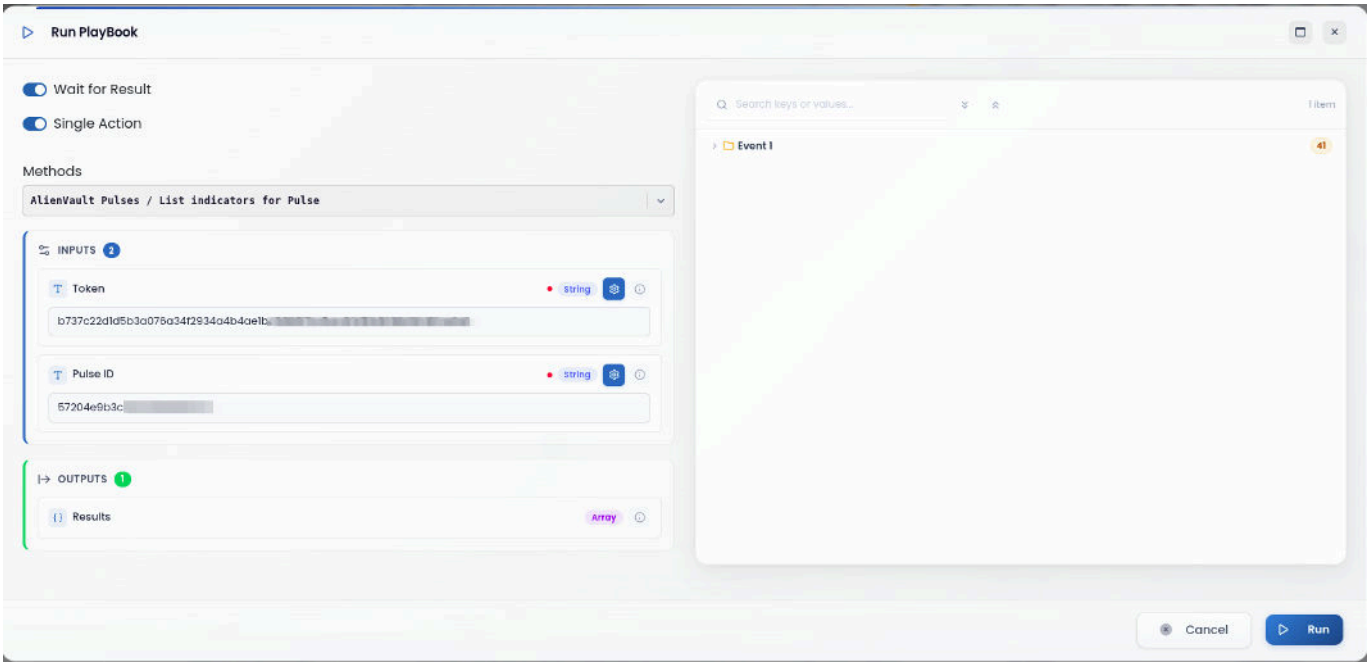


Inputs	Description
Token (is required)	To use the AlienVault API, you must have an API key
Pulse ID (is required)	The ID of Pulse

Outputs	Description
ID(id)	The ID of the interogated Pulse
Name(name)	The name of the Pulse
Description(description)	Details about Pulse
Author Name(author_name)	The name of the person/authority who created the Pulse
Modified(modified)	The timestamp when Pulse was last time modified
Created(created)	The timestamp when Pulse was created
Tags(tags)	A list which contains the tags added by the creator of the Pulse
References(references)	A collection of information containing references to various external sources relevant Pulse
Targeted Countries(targeted_countries)	A list which contains countries affected by the malware from the Pulse
Indicators(indicators)	Informations about the specific threat or security event which is investigated
Groups(groups)	A list which contains Open Source Threat Intelligence
Malware Families(malware_families)	A list containing the categories in which the malware was classified
Attack IDs(attack_ids)	A list which contains attack ids
Industries(industries)	A list containing possible industries affected by malware

AlienVault Pulses/List indicators for Pulse method

Returns paginated list view of the indicators inside the pulse pulse_id.

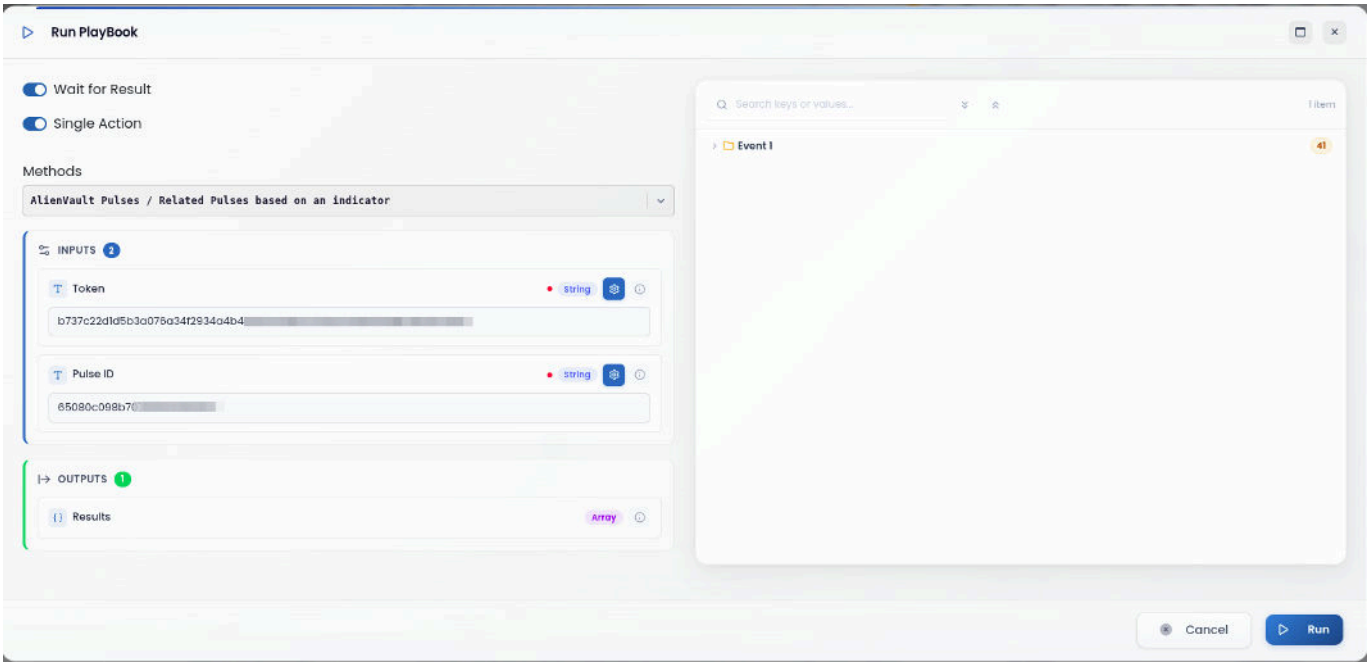


Inputs	Description
Token (is required)	To use the AlienVault API, you must have an API key
Pulse ID (is required)	The ID of Pulse that will be used

Outputs	Description
Results(results)	A list which contains reports for the Pulse based of API call

AlienVault Pulses/Related Pulses based on an indicator method

Return all pulses that share an indicator with this pulse.

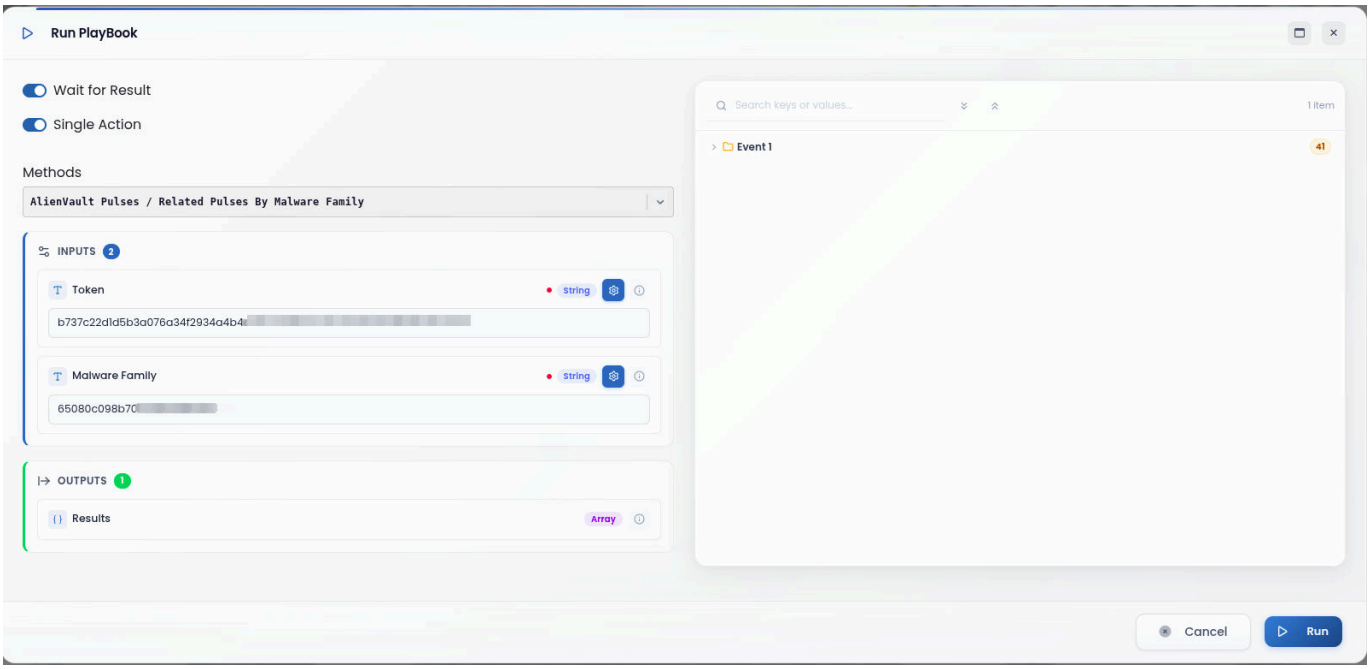


Inputs	Description
Token (is required)	To use the AlienVault API, you must have an API key
Pulse ID (is required)	The ID of Pulse that will be used

Outputs	Description
Results(results)	A list which contains reports for the Pulse based of API call

AlienVault Pulses/Related Pulses By Malware Family method

Find pulses related to either an existing a malware family.

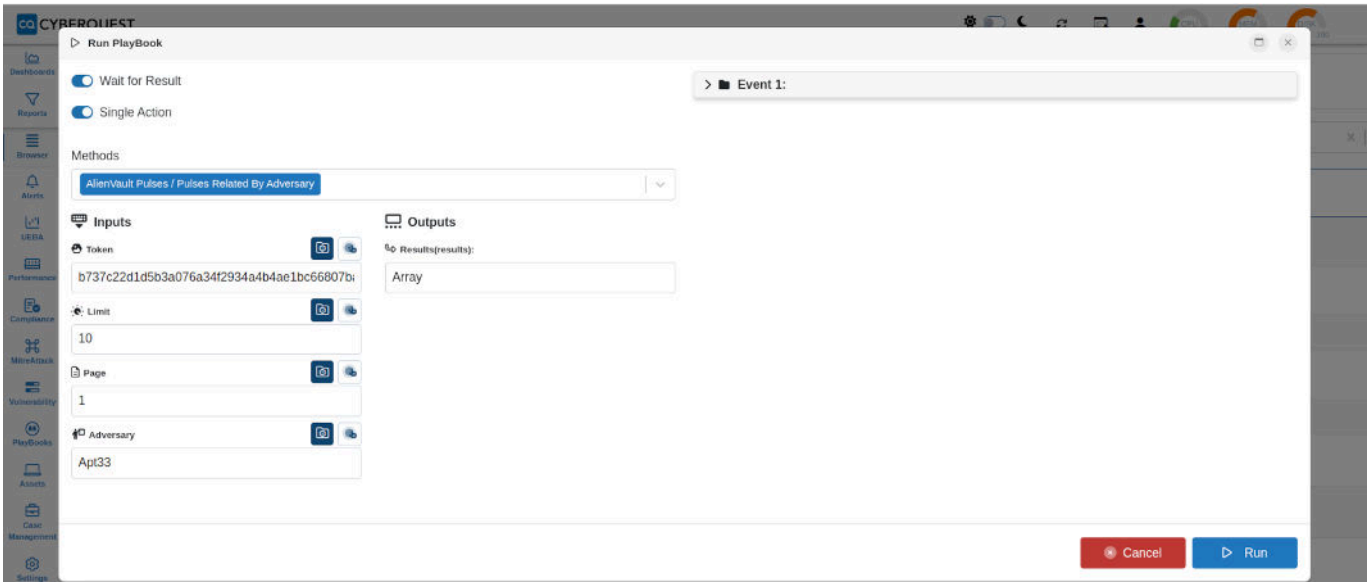


Inputs	Description
Token (is required)	To use the AlienVault API, you must have an API key
Malware Family (is required)	The malware family you'd like to find pulsed related to

Outputs	Description
Results(results)	A list which contains reports for the Pulse based of API call

AlienVault Pulses/Pulses Related By Adversary method

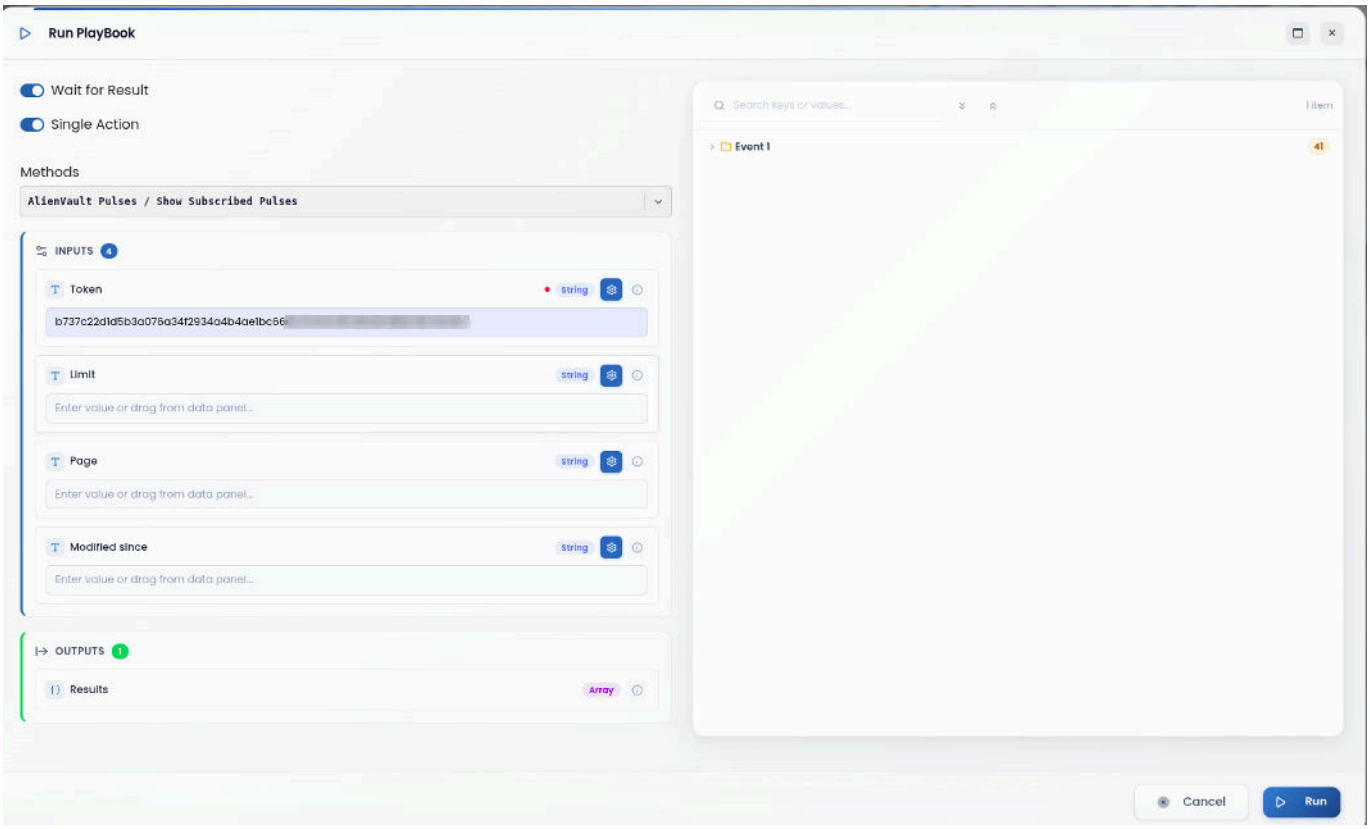
Find pulses related to either an existing an adversary.



Inputs	Description
Token (is required)	To use the AlienVault API, you must have an API key
Limit	Number of results to include per page
Page	Which page of results is desired
Adversary (is required)	Adversary you'd like to find pulsed related to

Outputs	Description
Results(results)	A list which contains reports for the Pulse based of API call

AlienVault Pulses/Show Subscribed Pulses method

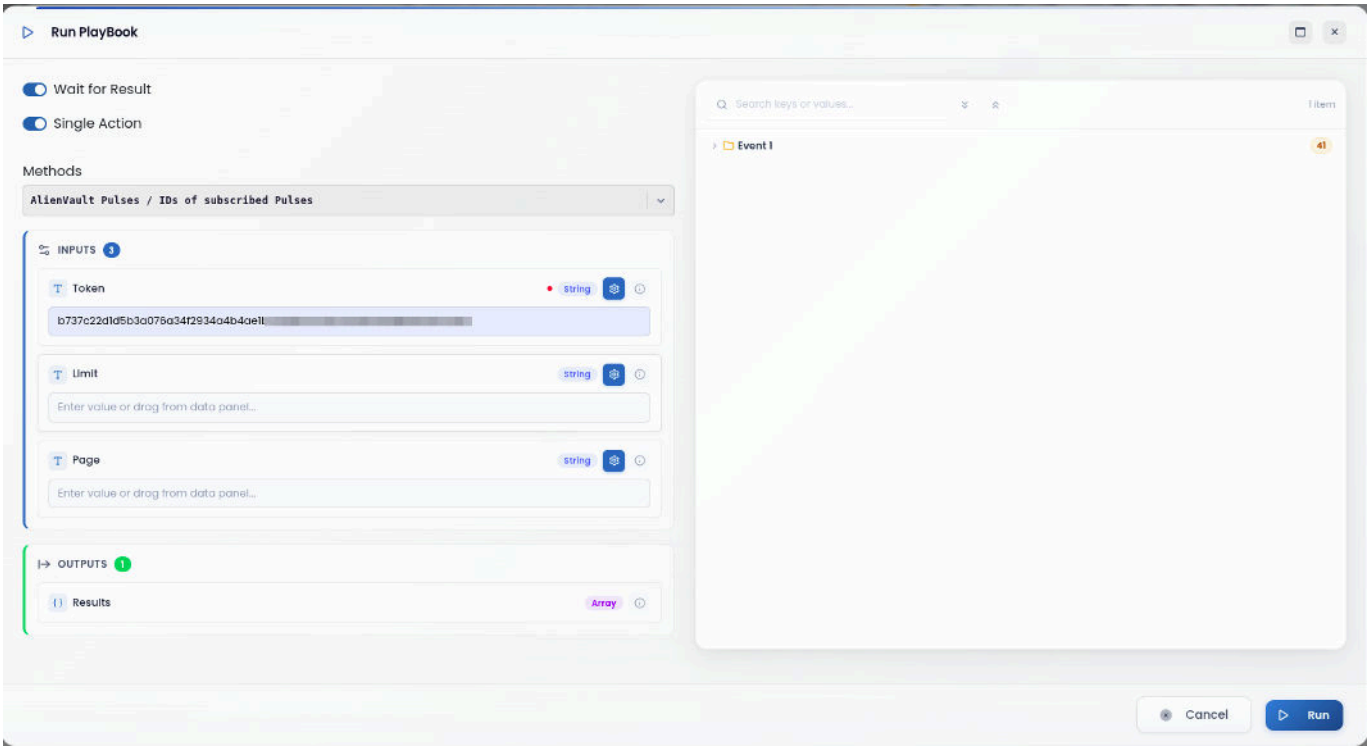


Inputs	Description
Token (is required)	To use the AlienVault API, you must have an API key
Limit	Number of results to include per page
Page	Which page of results is desired
Modified since	(optional, ISO format datetime (UTC) string) Only include pulses who is modified time is strictly greater than the supplied parameter. Accepts any valid ISO 8601 formatted datetime, with resolution up to and including milliseconds (for example 2017-01-01T12:35:00.123+00:00)

Outputs	Description
Results(results)	A list which contains reports for the Pulse based of API call

AlienVault Pulses/IDs of subscribed Pulses method

List the IDs of all pulses you are subscribed to.



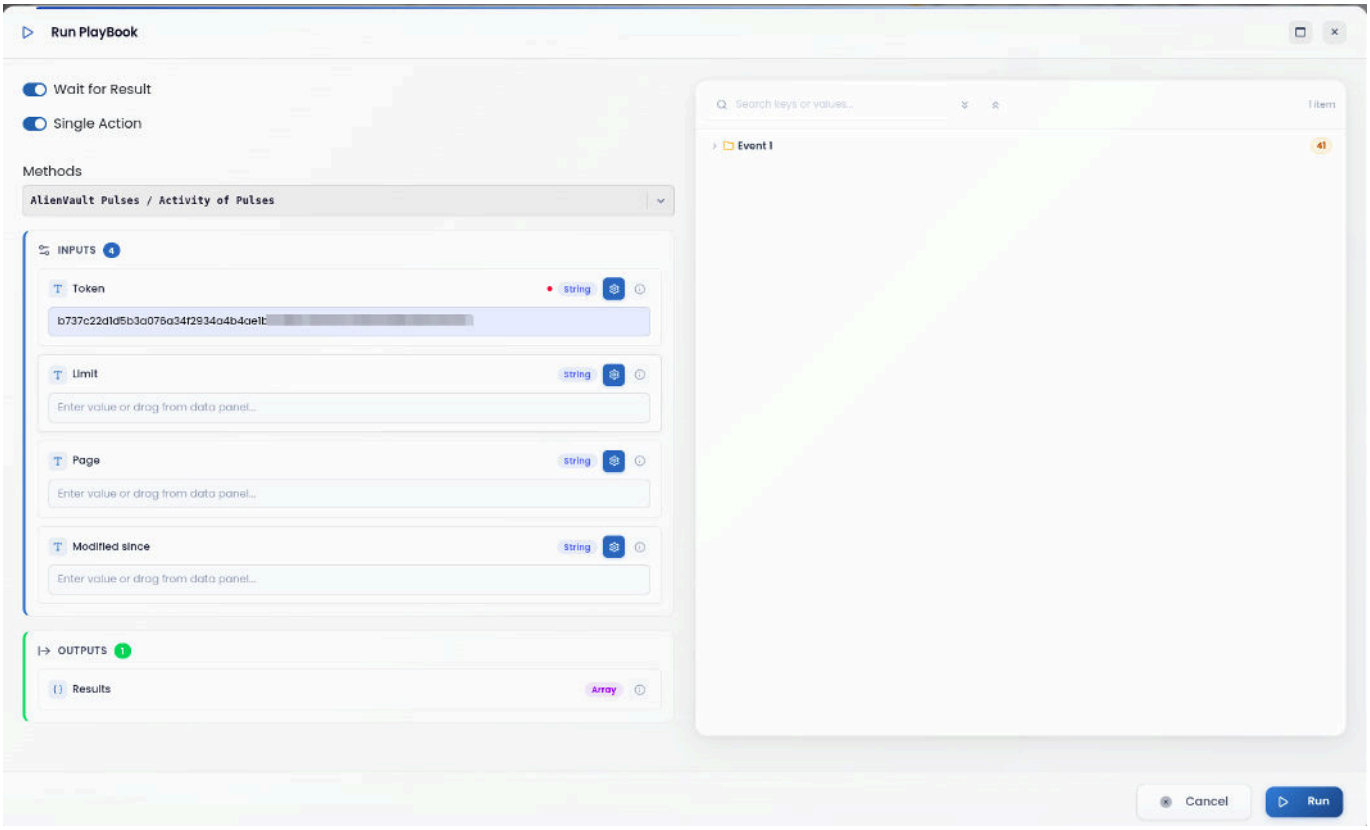
Inputs	Description
Token (is required)	To use the AlienVault API, you must have an API key
Limit	Number of results to include per page
Page	Which page of results is desired

Outputs	Description
Results(results)	A list which contains reports for the Pulse based of API call

AlienVault Pulses/Activity of Pulses method

Activity feed consists of pulses:

- All pulse subscriptions (directly subscribed to pulse, and all pulses by subscribed to users)
- All pulses created by myself
- All pulses by users I am following

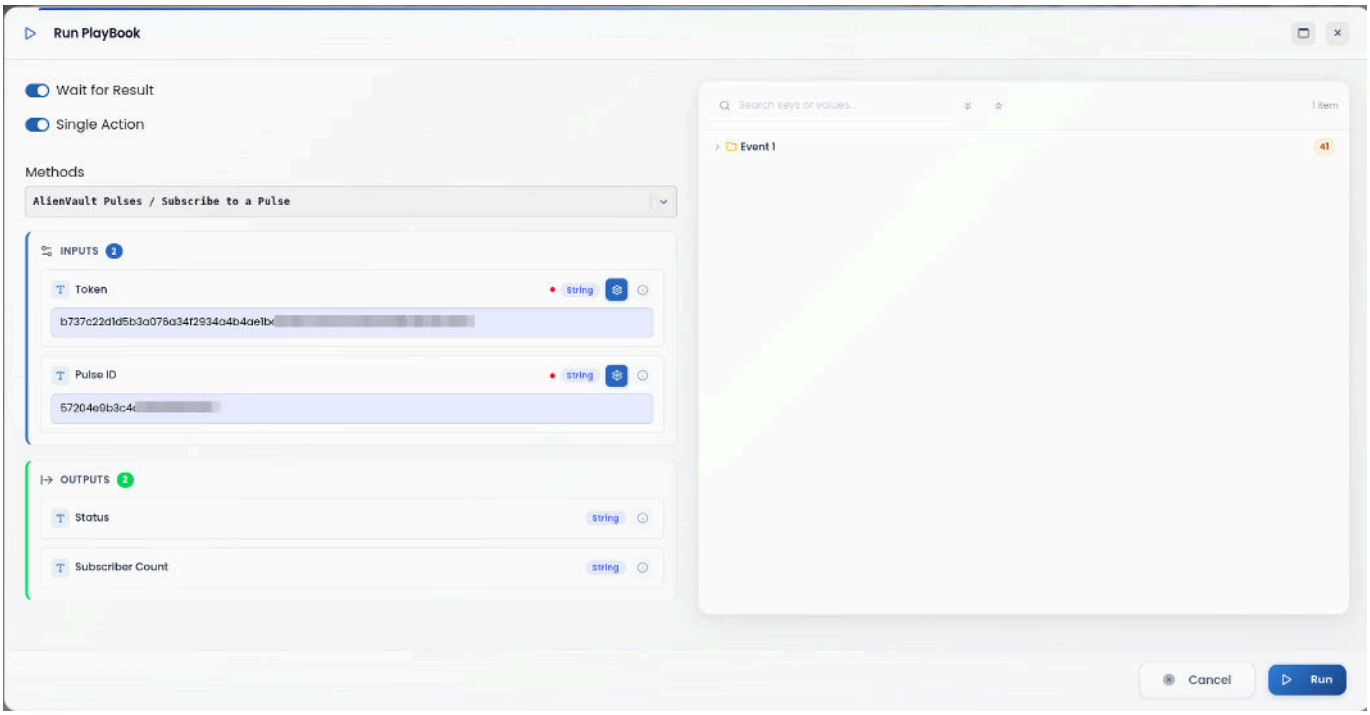


Inputs	Description
Token (is required)	To use the AlienVault API, you must have an API key
Limit	Number of results to include per page
Page	Which page of results is desired
Modified since	(optional, ISO 8601 format datetime (UTC) string) Only include pulses who is modified time is strictly greater than the supplied parameter. Accepts any valid ISO 8601 formatted datetime, with resolution up to and including milliseconds (for example 2017-01-01T12:35:00+00:00)

Outputs	Description
Results(results)	A list which contains reports for the Pulse based of API call

AlienVault Pulses/Subscribe to a Pulse method

Subscribe to pulse.

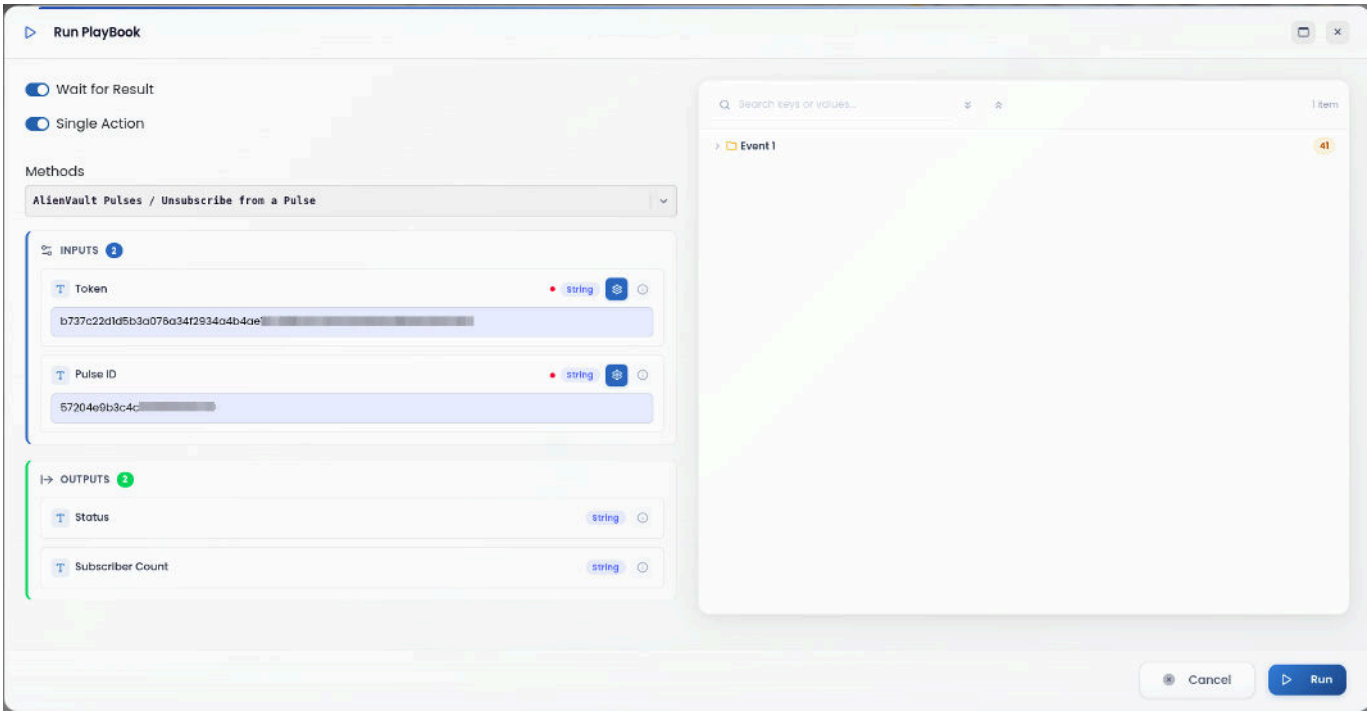


Inputs	Description
Token (is required)	To use the AlienVault API, you must have an API key
Pulse ID (is required)	The ID of Pulse the will be used

Outputs	Description
Status(status)	The status of the action
Subscriber Count(subscriber_count)	The number of subscribers of the Pulse

AlienVault Pulses/Unsubscribe from a Pulse method

Unsubscribe from pulse.

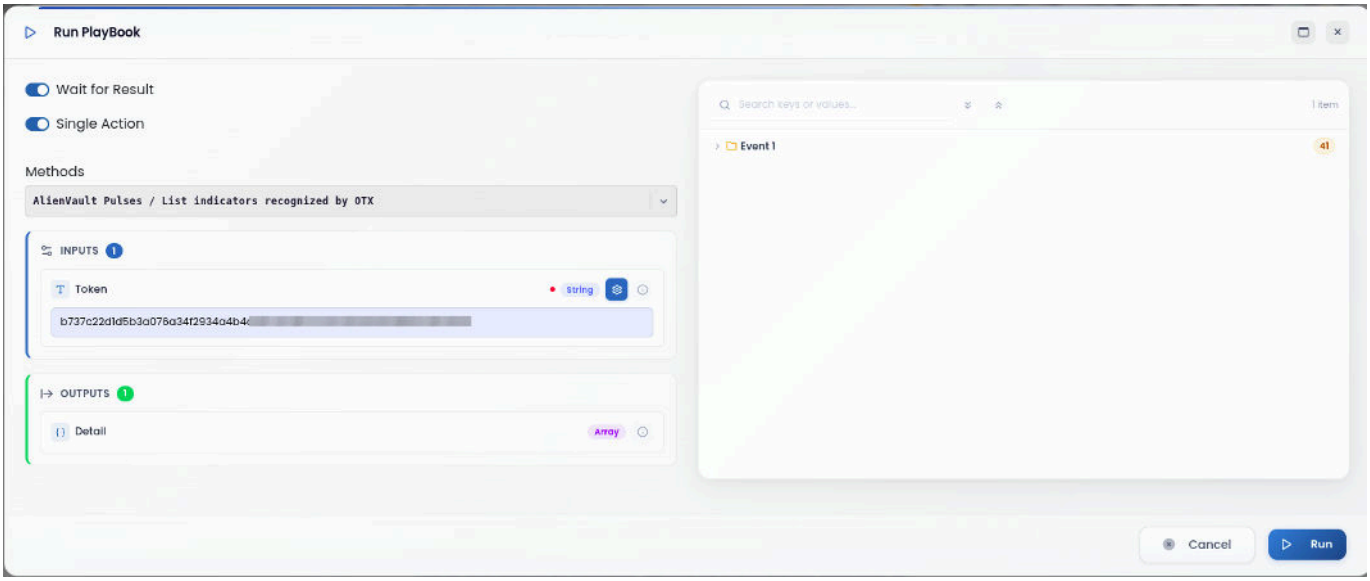


Inputs	Description
Token (is required)	To use the AlienVault API, you must have an API key
Pulse ID (is required)	The ID of Pulse the will be used

Outputs	Description
Status(status)	The status of the action
Subscriber Count(subscriber_count)	The number of subscribers of the Pulse

AlienVault Pulses/List indicators recognized by OTX method

Returns string representations of each indicator type (i.e. “domain”), as recognized by OTX.

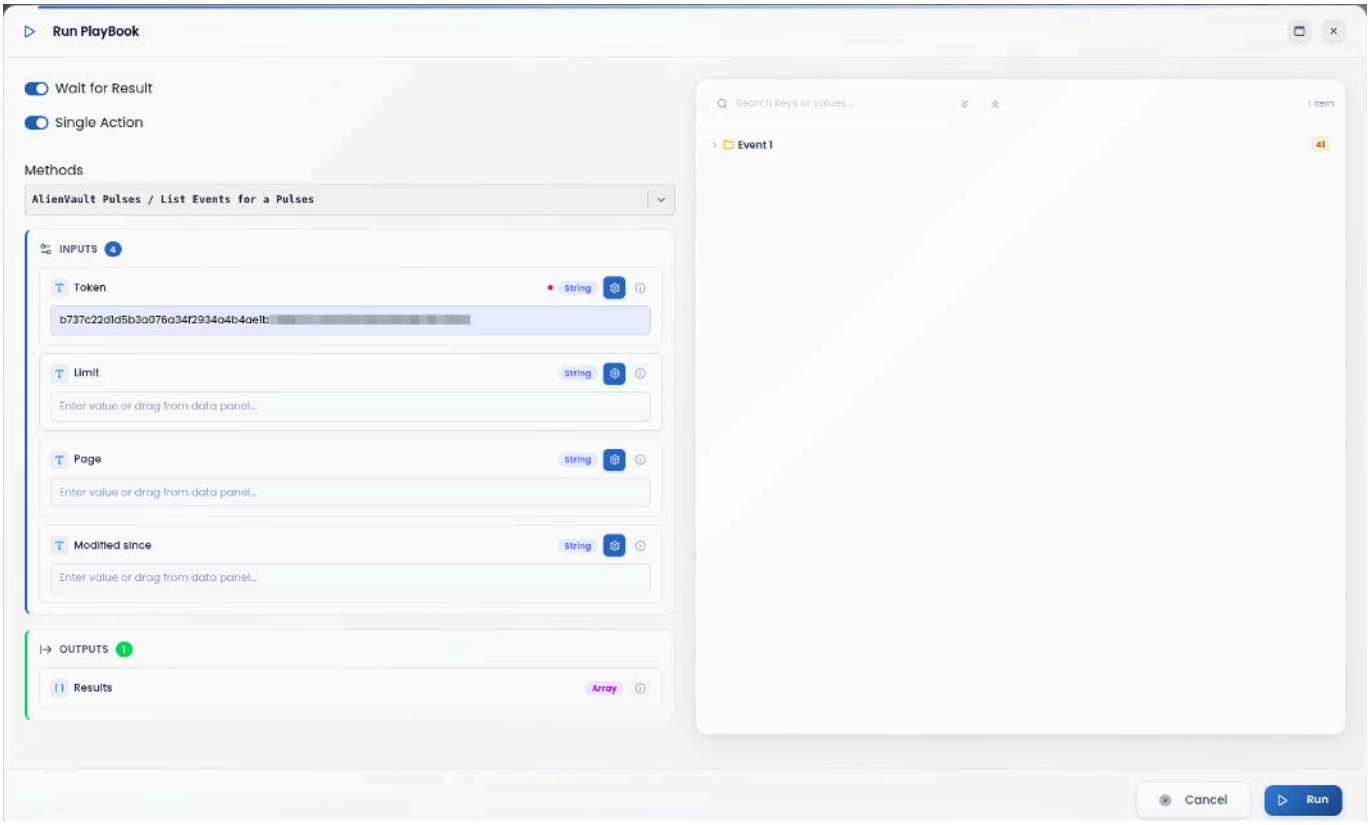


Inputs	Description
Token (is required)	To use the AlienVault API, you must have an API key

Outputs	Description
Detail(detail)	A list with indicators recognized by AlienVault

AlienVault Pulses/List Events for a Pulses method

List events, such as subscribe/unsubscribe to user/pulse.

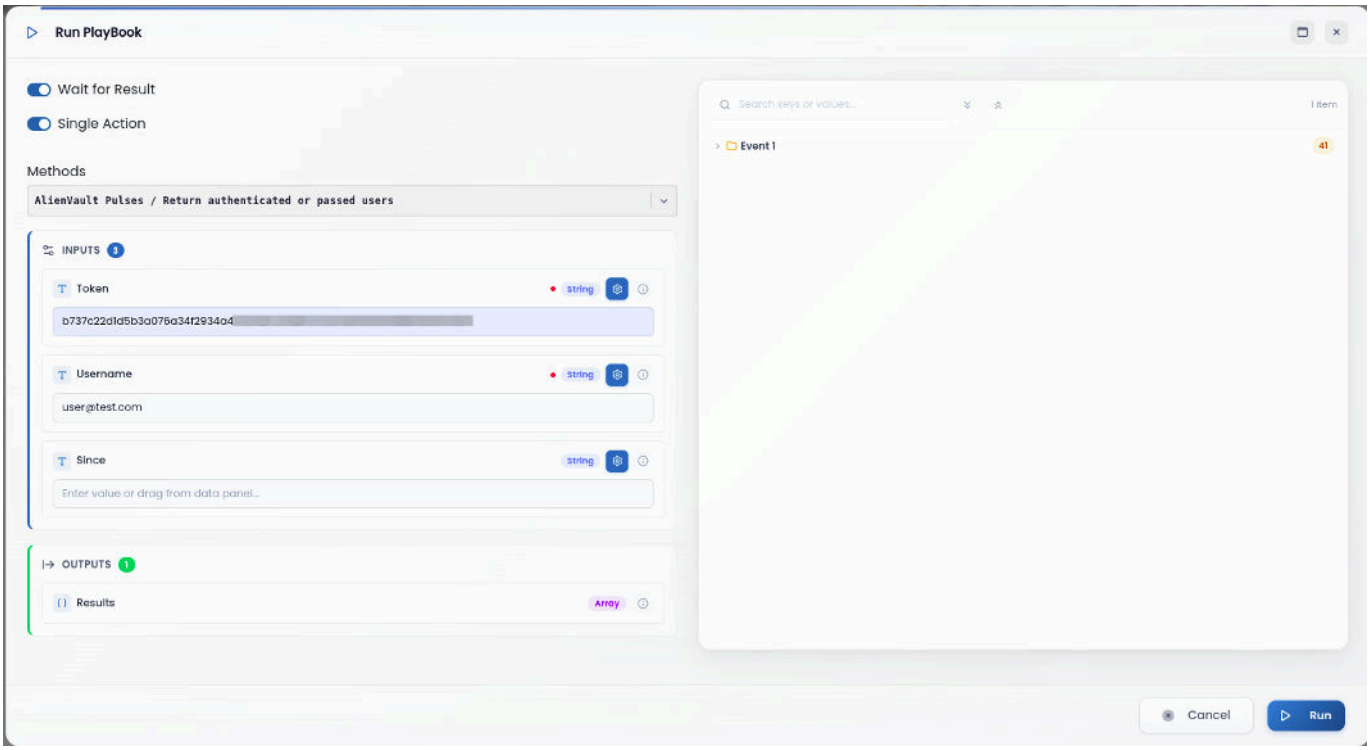


Inputs	Description
Token (is required)	To use the AlienVault API, you must have an API key
Limit	Number of results to include per page
Page	Which page of results is desired
Modified since	(optional, ISO format datetime (UTC) string) Only include pulses modified more recently than a specific time.

Outputs	Description
Results(results)	A list of events related to pulse

AlienVault Pulses/Return authenticated or passed users method

Returns authenticated users or passed in user created pulse feed, default sorted by latest modified.

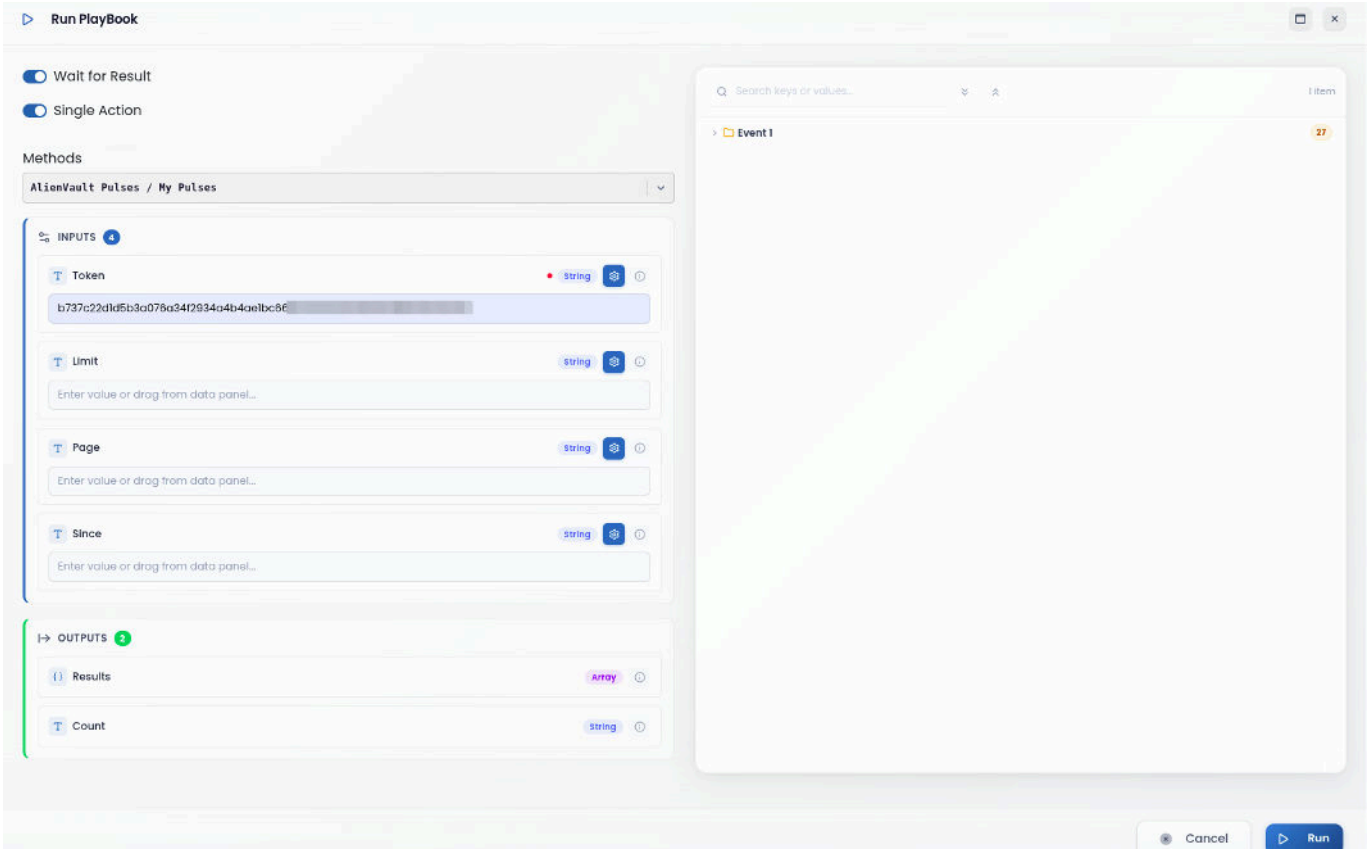


Inputs	Description
Token (is required)	To use the AlienVault API, you must have an API key
Username (is required)	Retrieve details about the username that will be introduced
Since	(optional, ISO format datetime (UTC) string) Only include pulses who has modified time is strictly greater than the supplied parameter. Accepts any valid ISO 8601 formatted datetime, with resolution up to and including milliseconds (for example 2017-01-01T12:35:00.123+00:00)

Outputs	Description
Results(results)	The results of the API call

AlienVault Pulses/My Pulses method

Returns your feed of pulses you've created, default sorted by latest modified.

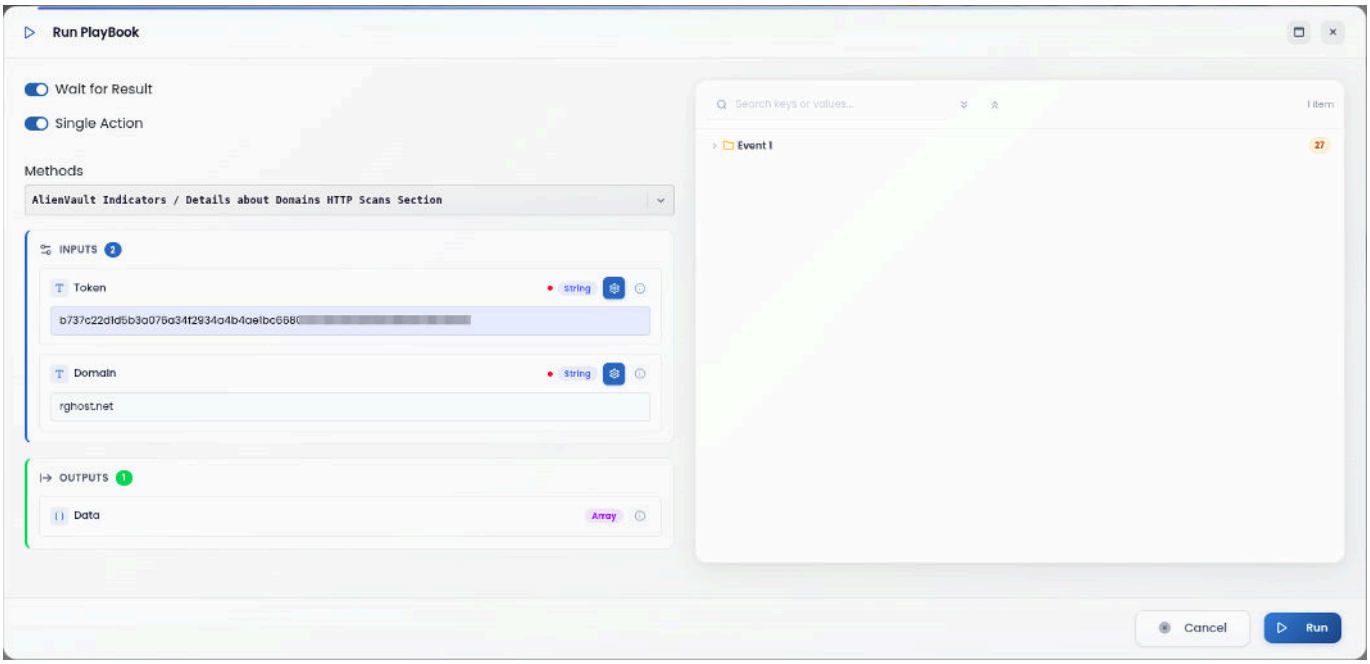


Inputs	Description
Token (is required)	To use the AlienVault API, you must have an API key
Limit	Number of results to include per page
Page	Which page of results is desired
Since	(optional, ISO format datetime (UTC) string) Only include pulses who has modified time is strictly greater than the supplied parameter. Accepts any valid ISO 8601 formatted datetime, with resolution up to and including milliseconds (for example 2017-01-01T12:35:00.123+00:00)

Outputs	Description
Results(results)	A list with pulses created by you
Count(count)	The number of pulses created by you

AlienVault Indicators/Details about Domains HTTP Scans Section method

Indicator page API for https scan section.

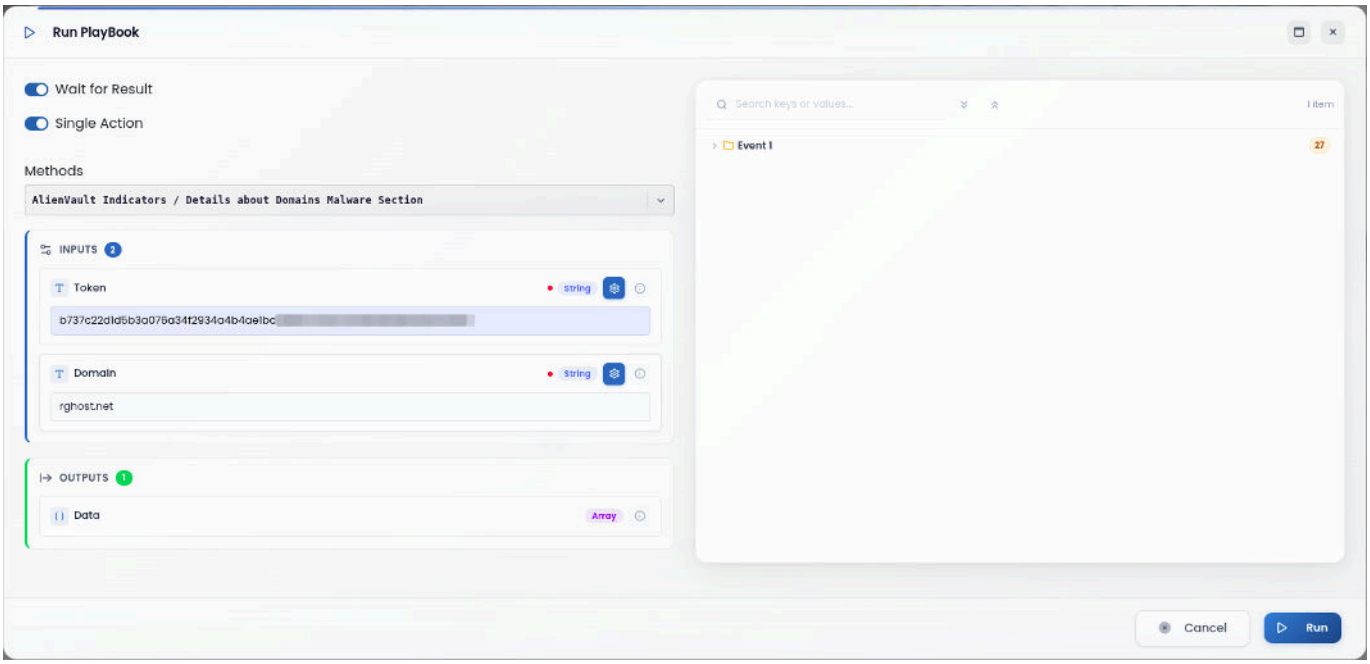


Inputs	Description
Token (is required)	To use the AlienVault API, you must have an API key
Domain (is required)	Retrieve details about domain that will be introduced

Outputs	Description
Data(data)	A list of reports for the intevestigated IP

AlienVault Indicators/Details about Domains Malware Section method

Indicator page API for malware section.

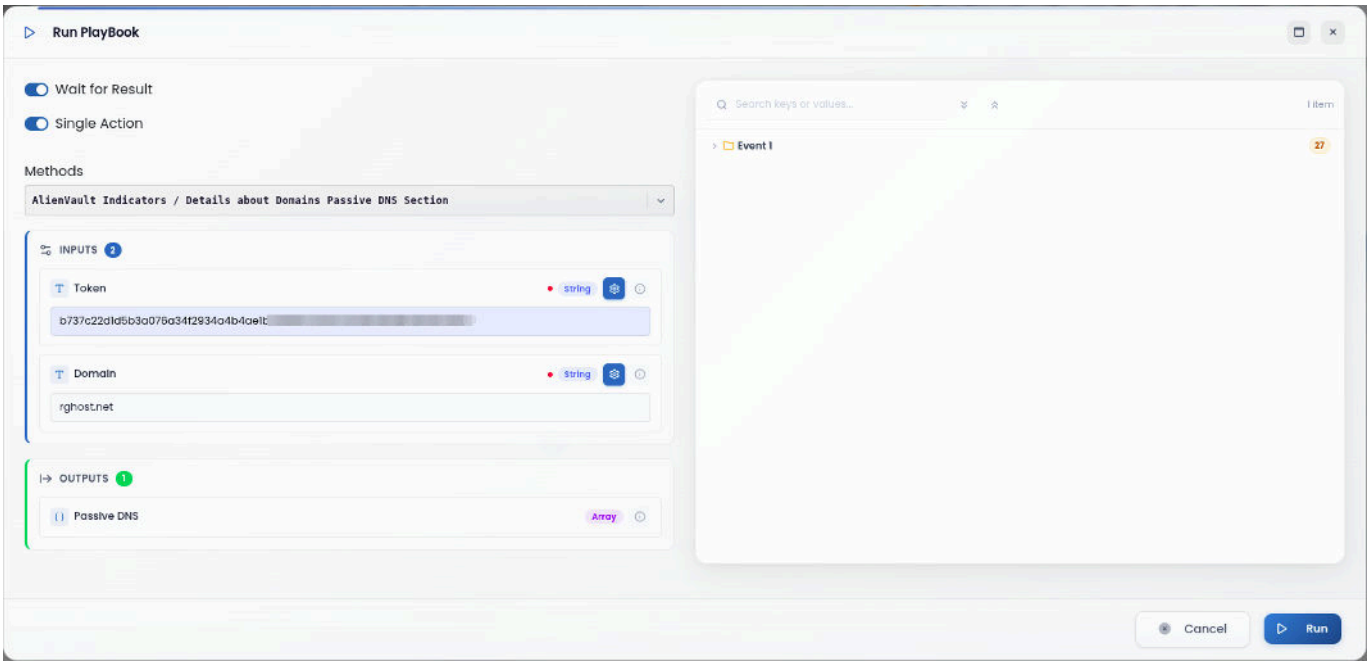


Inputs	Description
Token (is required)	To use the AlienVault API, you must have an API key
Domain (is required)	Retrieve details about domain that will be introduced

Outputs	Description
Data(data)	A list of reports for the intevestigated IP

AlienVault Indicators/Details about Domains Passive DNS Section method

Indicator page API for DNS section.

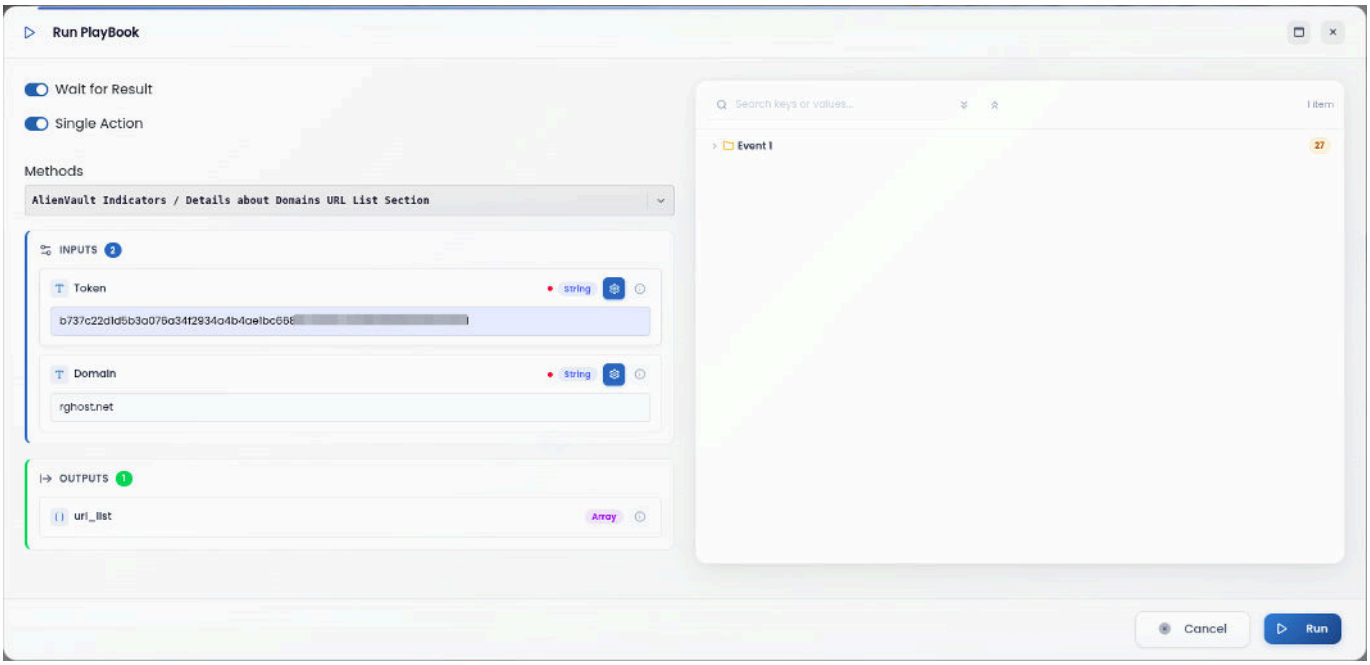


Inputs	Description
Token (is required)	To use the AlienVault API, you must have an API key
Domain (is required)	Retrieve details about domain that will be introduced

Outputs	Description
Passive DNS(passive_dns)	A list of reports for investigated domain

AlienVault Indicators/Details about Domains URL List Section method

Indicator page API for URL List section.

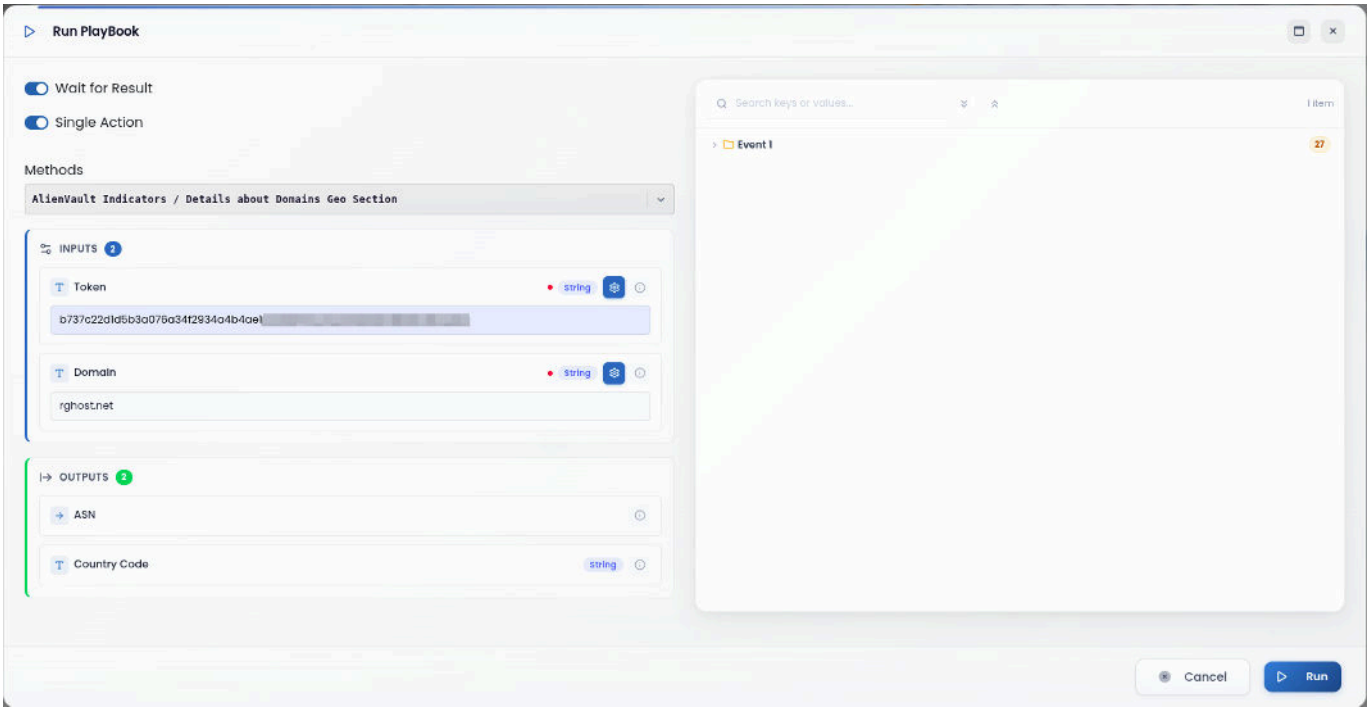


Inputs	Description
Token (is required)	To use the AlienVault API, you must have an API key
Domain (is required)	Retrieve details about domain that will be introduced

Outputs	Description
url_list(url_list)	The reports obtained after calling the API

AlienVault Indicators/Details about Domains Geo Section method

Indicator page API for Geo Section.

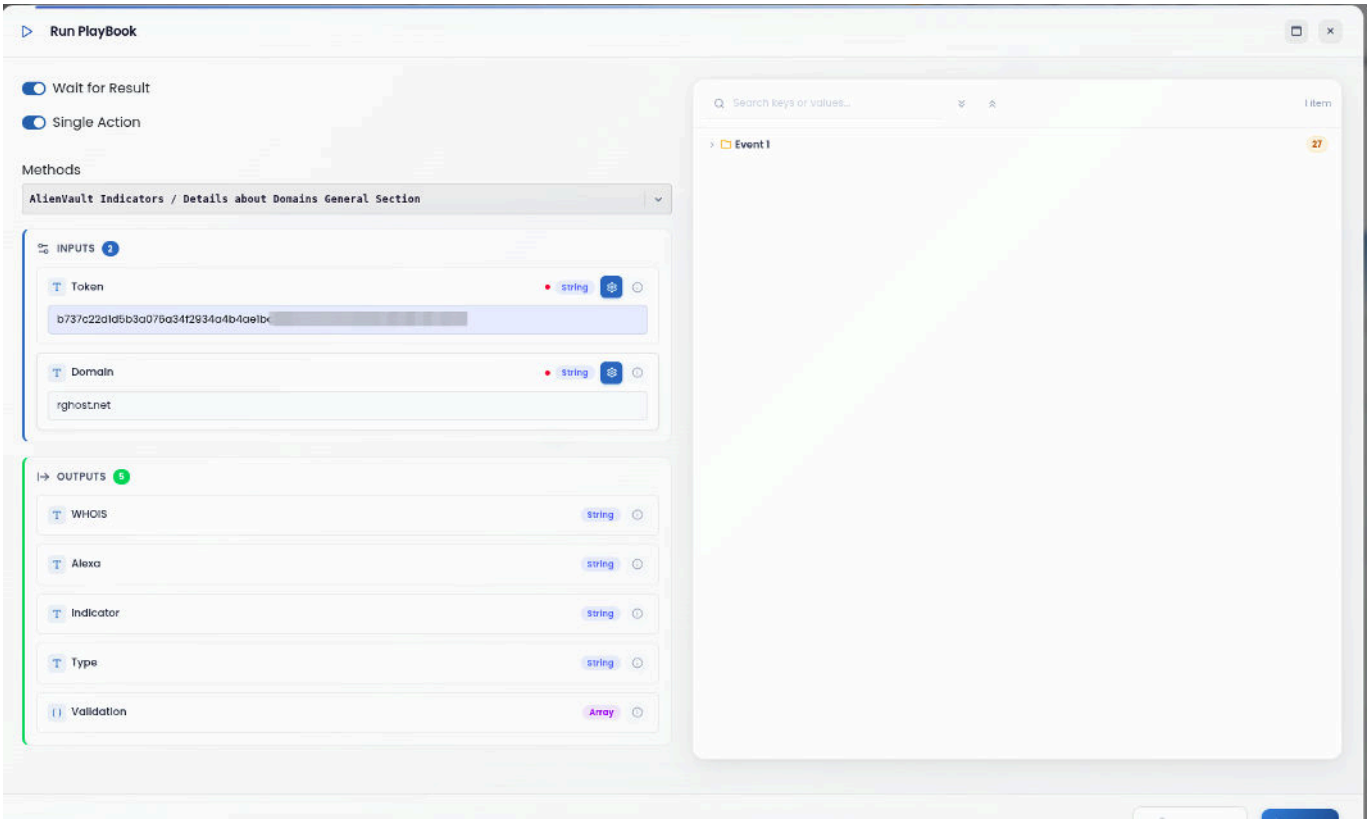


Inputs	Description
Token (is required)	To use the AlienVault API, you must have an API key
Domain (is required)	Retrieve details about domain that will be introduced

Outputs	Description
ASN(asn)	The name of ASN
Country Code(country_code)	The country name from where originates investigated IP

AlienVault Indicators/Details about Domains General Section method

Indicator page API for General section.

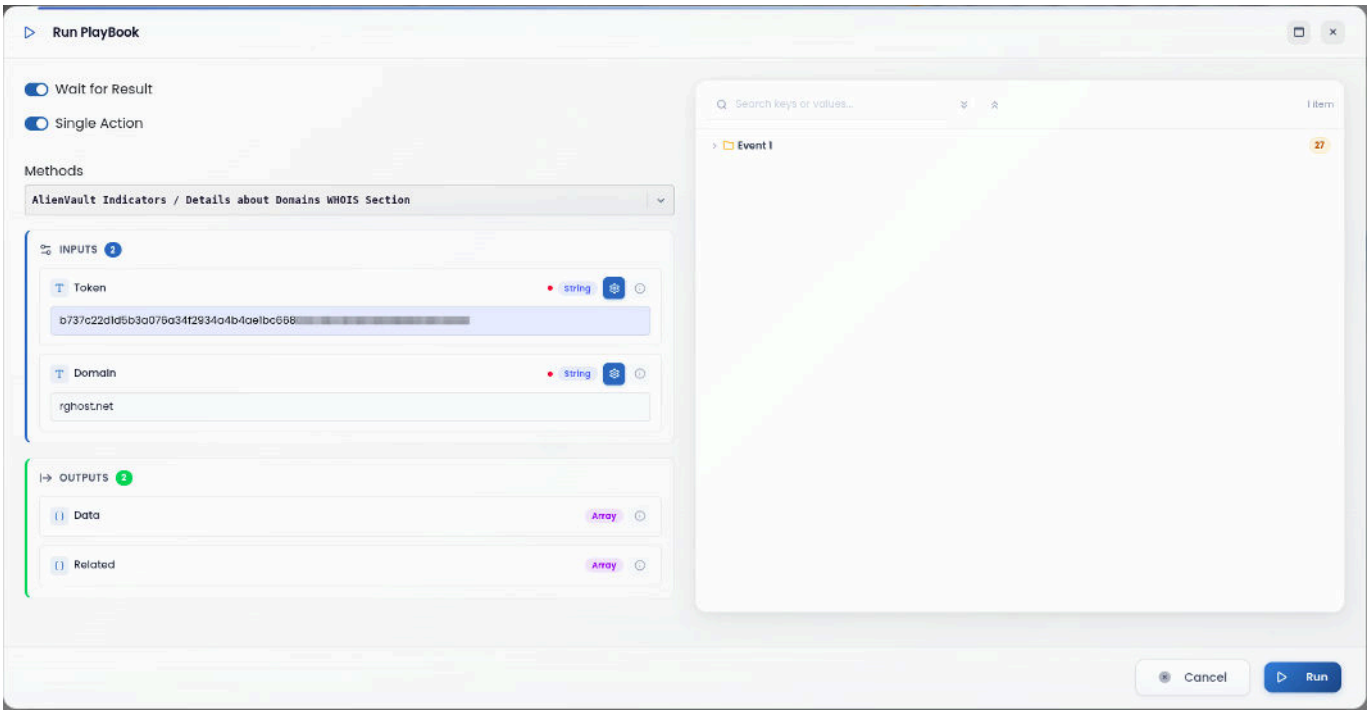


Inputs	Description
Token (is required)	To use the AlienVault API, you must have an API key
Domain (is required)	Retrieve details about domain that will be introduced

Outputs	Description
WHOIS(whois)	An external link to gain additional WHOIS informations
Alexa(alexa)	An external link to gain additional informations from Amazon Alexa
Indicator(indicator)	Informations about the specific threat or security event which is investigated
Type(type)	The type of the investigation
Validation(validation)	A list of validations done on the investigated domain

AlienVault Indicators/Details about Domains WHOIS Section method

Indicator page API for WHOIS section.

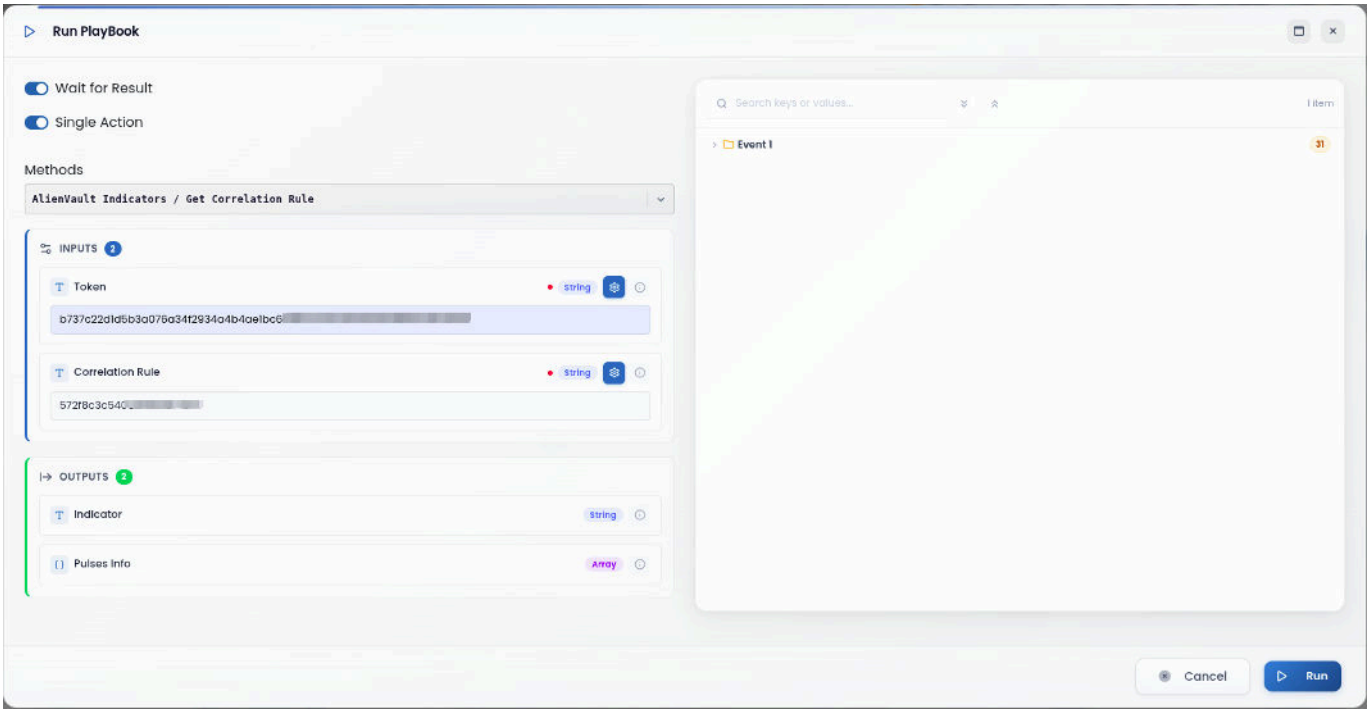


Inputs	Description
Token (is required)	To use the AlienVault API, you must have an API key
Domain (is required)	Retrieve details about domain that will be introduced

Outputs	Description
Data(data)	A list of reports for the intevestigated domain
Related(related)	A list of domains related to the investigated domain

AlienVault Indicators/Get Correlation Rule method

Indicator page API for Correlation Rules.

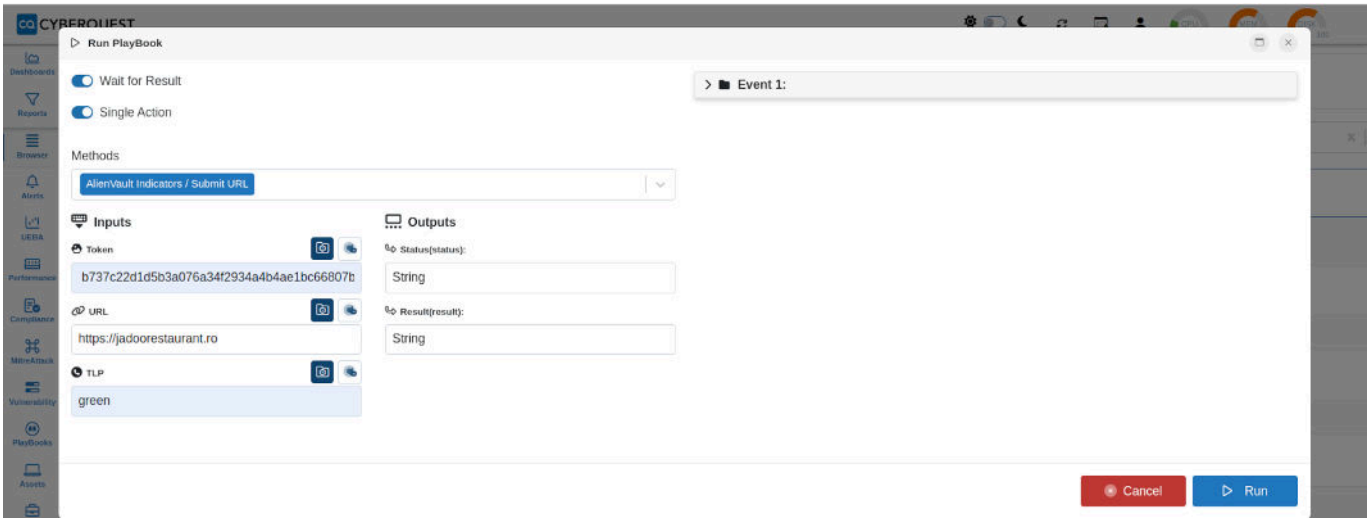


Inputs	Description
Token (is required)	To use the AlienVault API, you must have an API key
Correlation Rule (is required)	Correlation rules in AlienVault are used to analyze and correlate data from various security data sources, such as logs, network traffic, and vulnerability scans

Outputs	Description
Indicator(indicator)	Indicator (Correlation Rule from input parameter) link related events to detect security threats
Pulses Info(pulses)	Threat summaries available in the AlienVault Open Threat Exchange (OTX).

AlienVault Indicators/Submit URL method

This is an endpoint to Submit a single URL at once.

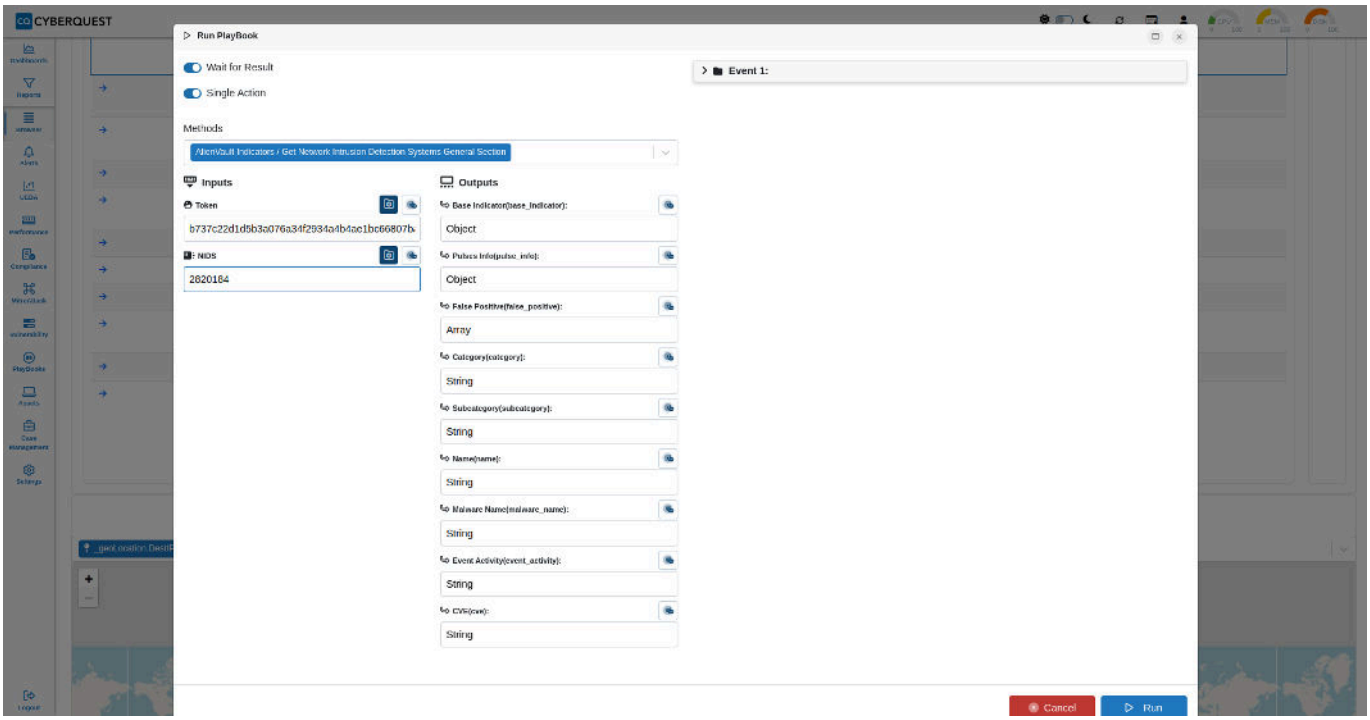


Inputs	Description
Token (is required)	To use the AlienVault API, you must have an API key
URL (is required)	The url that will be submitted
TLP (is required)	Select the color of TLP for the url that will be submitted

Outputs	Description
Status(status)	The status of API call
Result(result)	The result of analysis

AlienVault Indicators/Get Network Intrusion Detection Systems General Section method

Indicator page API for NIDSs.

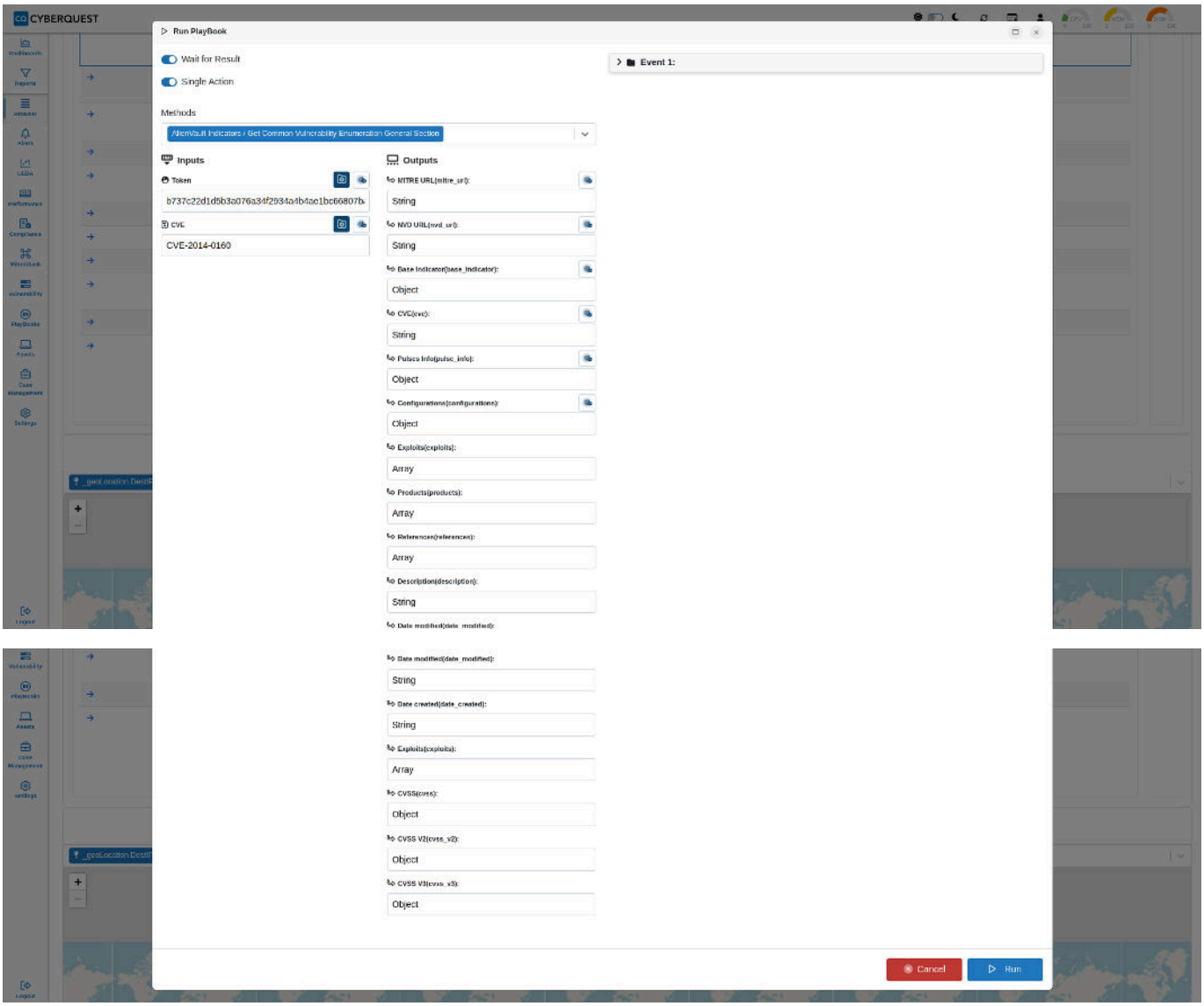


Inputs	Description
Token (is required)	To use the AlienVault API, you must have an API key
NIDS (is required)	Retrieve details about NIDS that will be introduced

Outputs	Description
Base Indicator(base_indicator)	Essential information about the specific threat or security event which is investigated
Pulses Info(pulse_info)	Threat summaries available in the AlienVault Open Threat Exchange (OTX)
False Positive(false_positive)	An Array which includes the false positives detected
Category(category)	The main category of security event detected by NIDS
Subcategory(subcategory)	Additional details about security event detected by NIDS
Name(name)	The name of the security event
Malware Name(malware_name)	The malware category in which is classified the security event
Event Activity(event_activity)	Details security event
CVE(cve)	CVE (Common Vulnerabilities and Exposures) is a program that assigns unique identifiers to publicly disclosed cybersecurity vulnerabilities

AlienVault Indicators/Get Common Vulnerability Enumeration General Section method

Indicator page API for CVEs (MITRE's Common Vulnerability Enumeration).

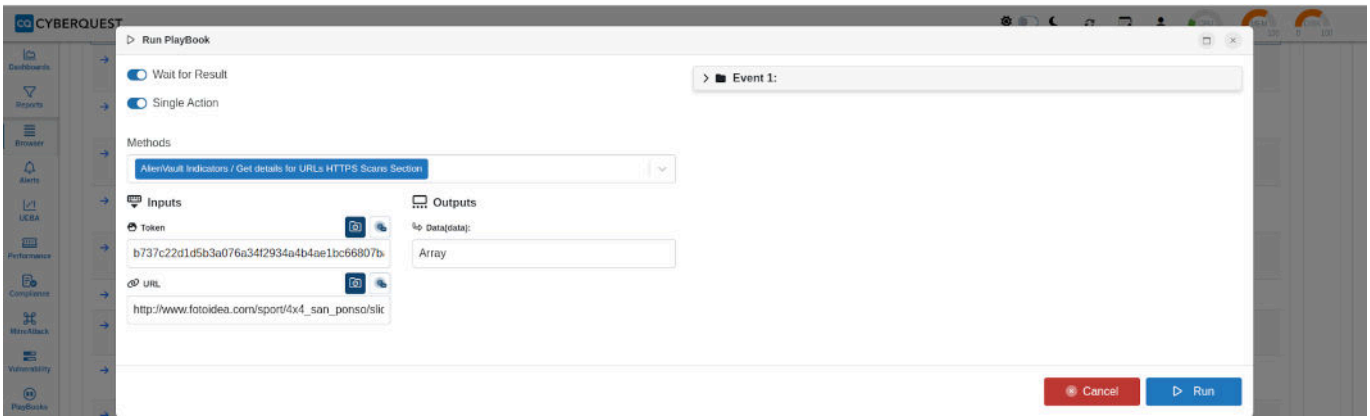


Inputs	Description
Token (is required)	To use the AlienVault API, you must have an API key
CVE (is required)	Retrieve details about CVE (Common Vulnerabilities and Exposures) that will be introduced

Outputs	Description
MITRE URL(mitre_url)	The Mitre URL to CVE ID investigated
NVD URL(nvd_url)	The NDV URL to CVE ID investigated
Base Indicator(base_indicator)	Essential information about the specific threat or security event which is investigated
CVE(cve)	CVE ID which is investigated
Pulses Info(pulse_info)	Threat summaries available in the AlienVault Open Threat Exchange (OTX).
Configurations(configurations)	The configurations used to test the CVE
Exploits(exploits)	A structured set of data containing information about vulnerabilities
Products(products)	A structured set of data containing information about affected products
References(references)	A collection of information containing references to various external sources relevant to the CVE investigated
Description(description)	General description about
Date modified(date_modified)	The last timestamp when the report was modified
Date created(date_created)	The timestamp when the report was created
CVSS(cvss)	Common Vulnerability Scoring System
CVSS V2(cvss_v2)	Common Vulnerability Scoring System Version 2
CVSS V3(cvss_v3)	Common Vulnerability Scoring System Version 3

AlienVault Indicators/Get details for URLs HTTPS Scans Section method

Indicator page API for URLs.

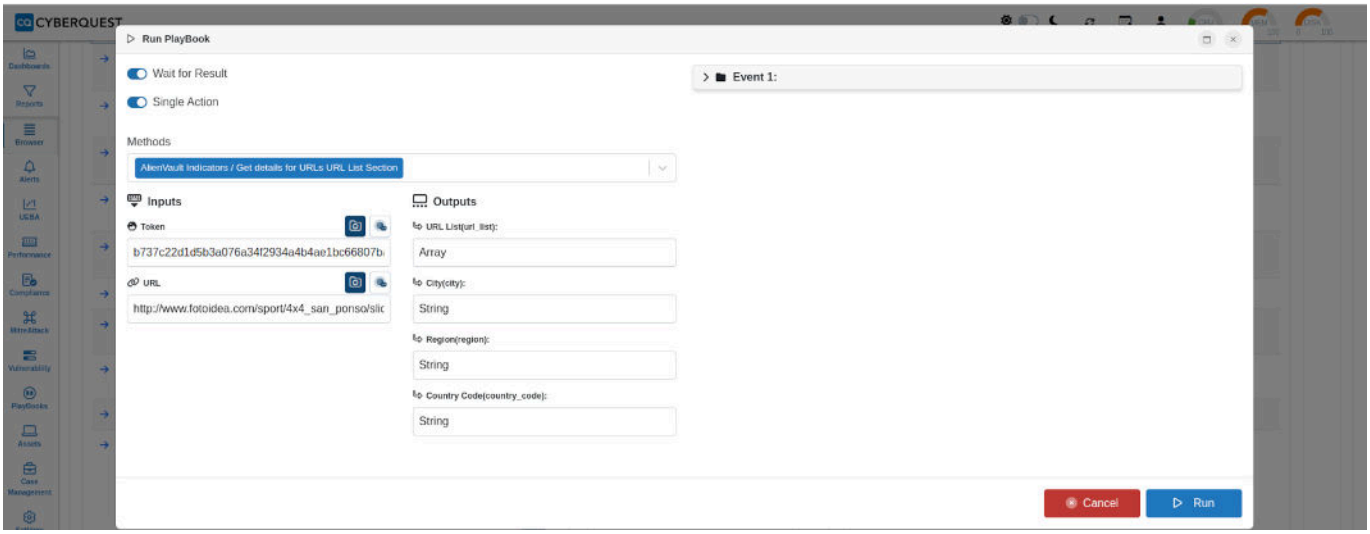


Inputs	Description
Token (is required)	To use the AlienVault API, you must have an API key
URL (is required)	Retrieve details about URL that will be introduced

Outputs	Description
Data(data)	The results of the API call which contains

AlienVault Indicators/Get details for URLs URL List Section method

Indicator page API for URLs.

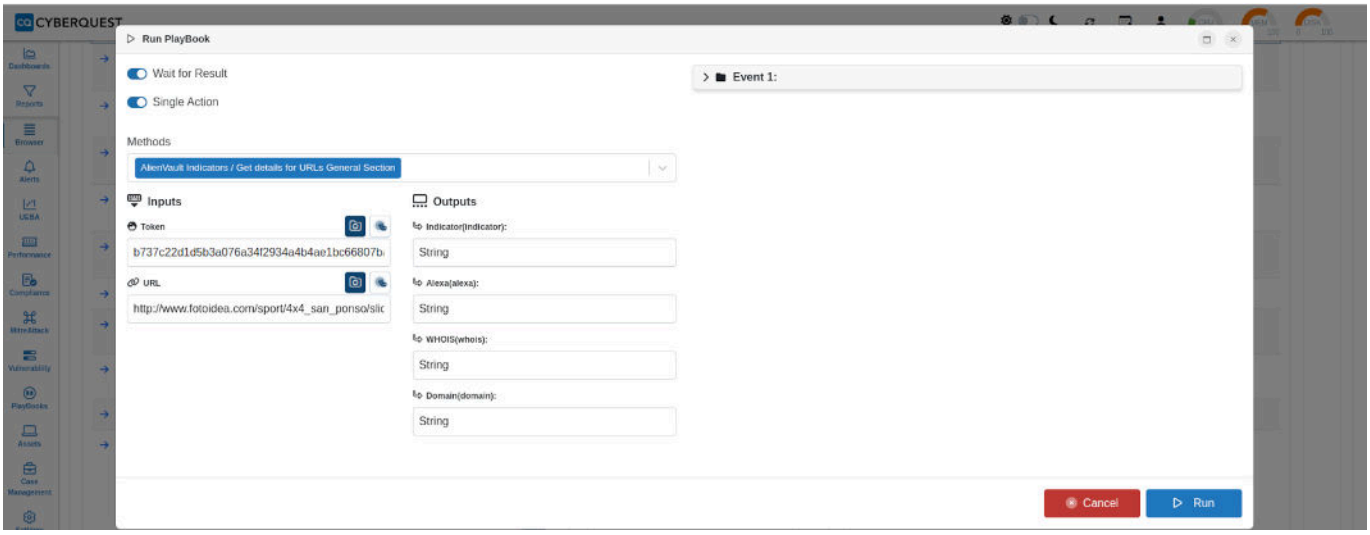


Inputs	Description
Token (is required)	To use the AlienVault API, you must have an API key
URL (is required)	Retrieve details about URL that will be introduced

Outputs	Description
URL List(url_list)	The reports obtained after calling the API
City(city)	The city from where originates investigated URL
Region(region)	The region from where originates investigated URL
Country Code(country_code)	The country code from where originates investigated URL

AlienVault Indicators/Get details for URLs General Section method

Indicator page API for URLs.

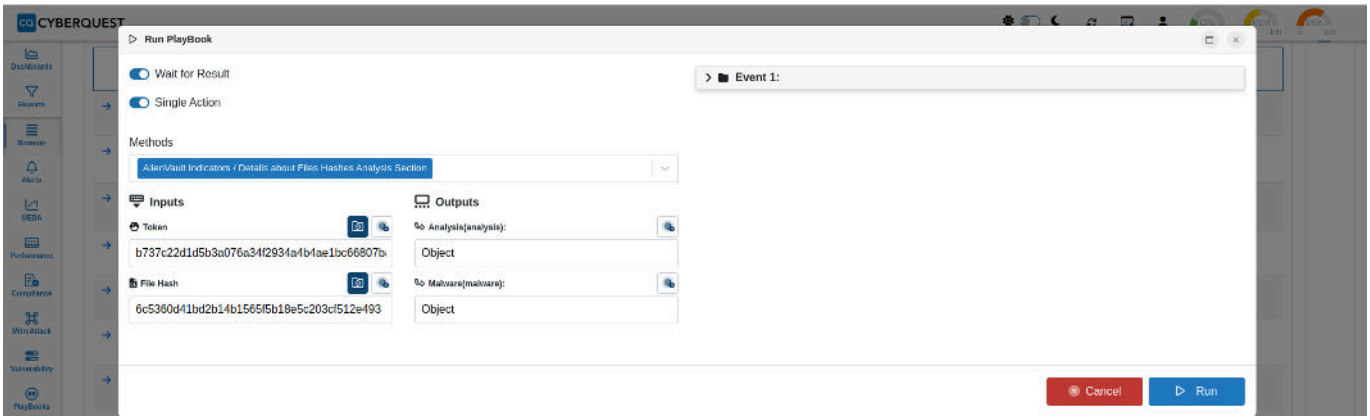


Inputs	Description
Token (is required)	To use the AlienVault API, you must have an API key
URL (is required)	Retrieve details about URL that will be introduced

Outputs	Description
Indicator(indicator)	Informations about the specific threat or security event which is investigated
Alexa(alexa)	An external link to gain additional informations from Amazon Alexa
WHOIS(whois)	An external link to gain additional WHOIS informations
Domain(domain)	The domain name of the investigated URL

AlienVault Indicators/Details about Files Hashes Analysis Section method

Indicator page API for files (file hashes).

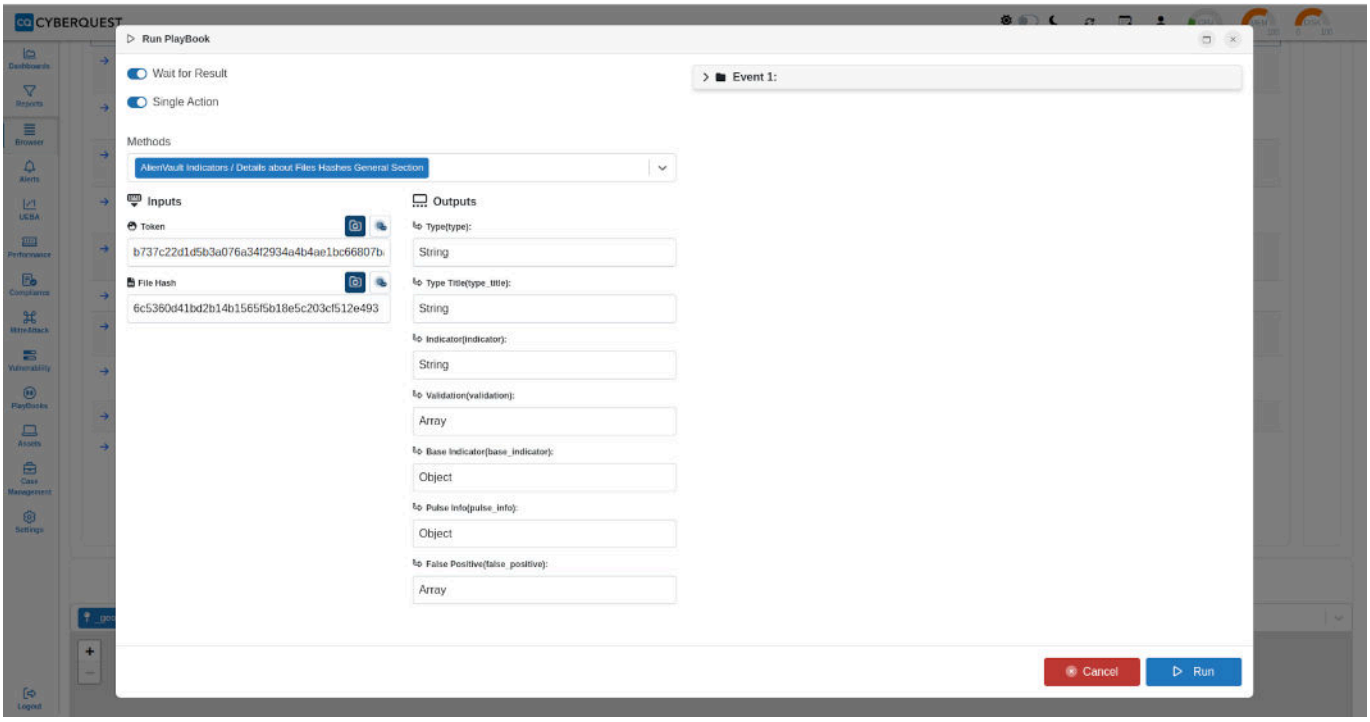


Inputs	Description
Token (is required)	To use the AlienVault API, you must have an API key
File Hash (is required)	Retrieve details about file hash that will be introduced

Outputs	Description
Analysis (analysis)	The result of the investigation
Malware (malware)	The possible types of malware detected

AlienVault Indicators/Details about Files Hashes General Section method

Indicator page API for files (file hashes).

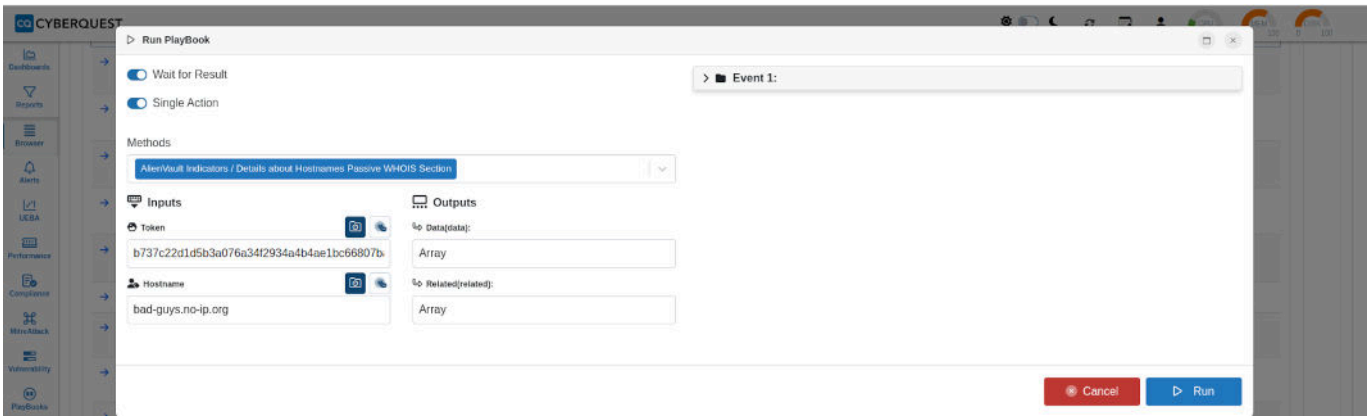


Inputs	Description
Token (is required)	To use the AlienVault API, you must have an API key
File Hash (is required)	Retrieve details about file hash that will be introduced

Outputs	Description
Type (type)	The type of the investigated hash
Type Title (type_title)	The full name of the investigated hash
Indicator (indicator)	Informations about the specific threat or security event which is investigated
Validation (validation)	A list of validations done on the investigated hash
Base Indicator (base_indicator)	Essential information about the specific threat or security event which is investigated
Pulse Info (pulse_info)	Threat summaries available in the AlienVault Open Threat Exchange (OTX).
False Positive (false_positive)	An Array which includes the false positives detected

AlienVault Indicators/Details about Hostnames Passive WHOIS Section method

Indicator page API for hostname names.

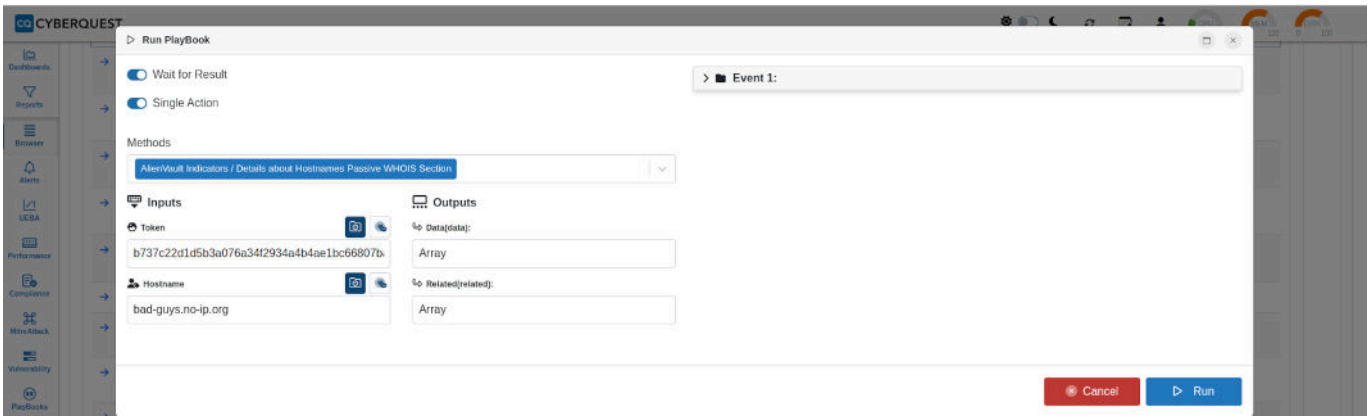


Inputs	Description
Token (is required)	To use the AlienVault API, you must have an API key
Hostname (is required)	Retrieve details about hostname that will be introduced

Outputs	Description
Data(data)	A list of reports for investigated hostname
Related(related)	A list of hostnames related to the investigated hostname

AlienVault Indicators/Details about Hostnames Passive Malware Section method

Indicator page API for hostname names.

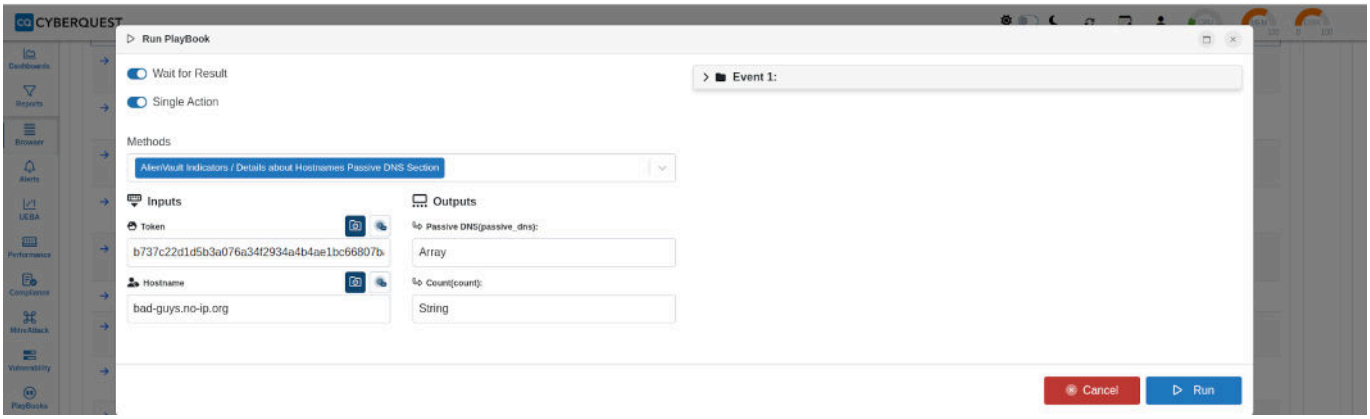


Inputs	Description
Token (is required)	To use the AlienVault API, you must have an API key
Hostname (is required)	Retrieve details about hostname that will be introduced

Outputs	Description
Data(data)	A list of reports for investigated hostname
Count(count)	A list of reports for investigated hostname

AlienVault Indicators/Details about Hostnames Passive DNS Section method

Indicator page API for hostname names.

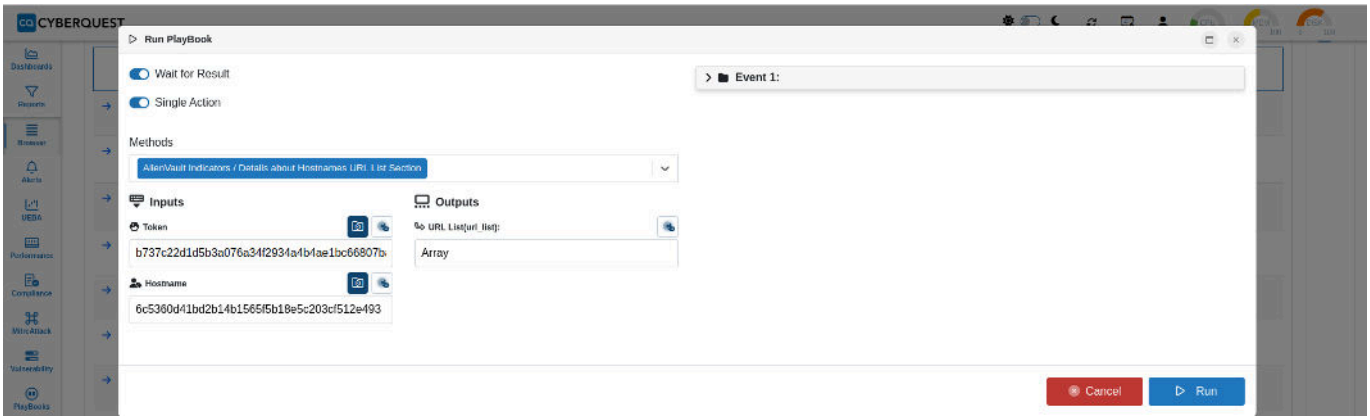


Inputs	Description
Token (is required)	To use the AlienVault API, you must have an API key
Hostname (is required)	Retrieve details about hostname that will be introduced

Outputs	Description
Passive DNS(passive_dns)	A list of reports for investigated hostname
Count(count)	The number of reports for the investigated hostname

AlienVault Indicators/Details about Hostnames URL List Section method

Indicator page API for hostname names.

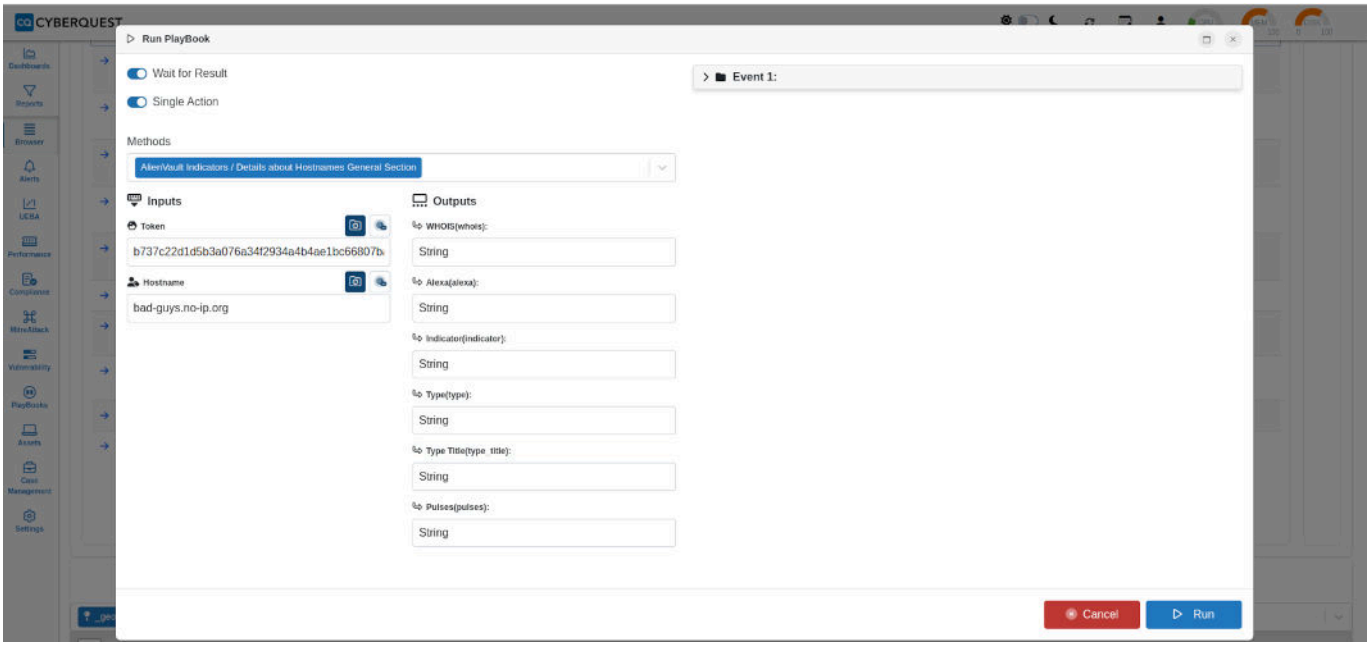


Inputs	Description
Token (is required)	To use the AlienVault API, you must have an API key
Hostname (is required)	Retrieve details about hostname that will be introduced

Outputs	Description
URL List(url_list)	The reports obtained after calling the API

AlienVault Indicators/Details about Hostnames General Section method

Indicator page API for hostname names.

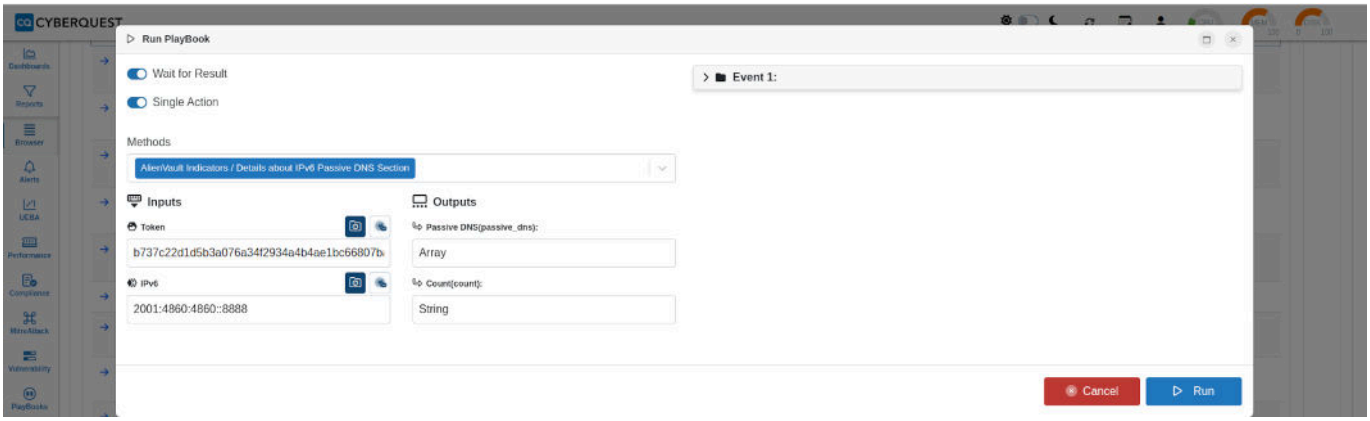


Inputs	Description
Token (is required)	To use the AlienVault API, you must have an API key
Hostname (is required)	Retrieve details about hostname that will be introduced

Outputs	Description
WHOIS (whois)	An external link to gain additional WHOIS informations
Alexa (alexa)	An external link to gain additional informations from Amazon Alexa
Indicator (indicator)	Informations about the specific threat or security event which is investigated
Type (type)	The type of the investigated hash
Type Title (type_title)	The full name of the investigated hash
Pulses (pulses)	Threat summaries available in the AlienVault Open Threat Exchange (OTX)

AlienVault Indicators/Details about IPv6 Passive DNS Section method

Indicator page API for IPv6 Addresses.

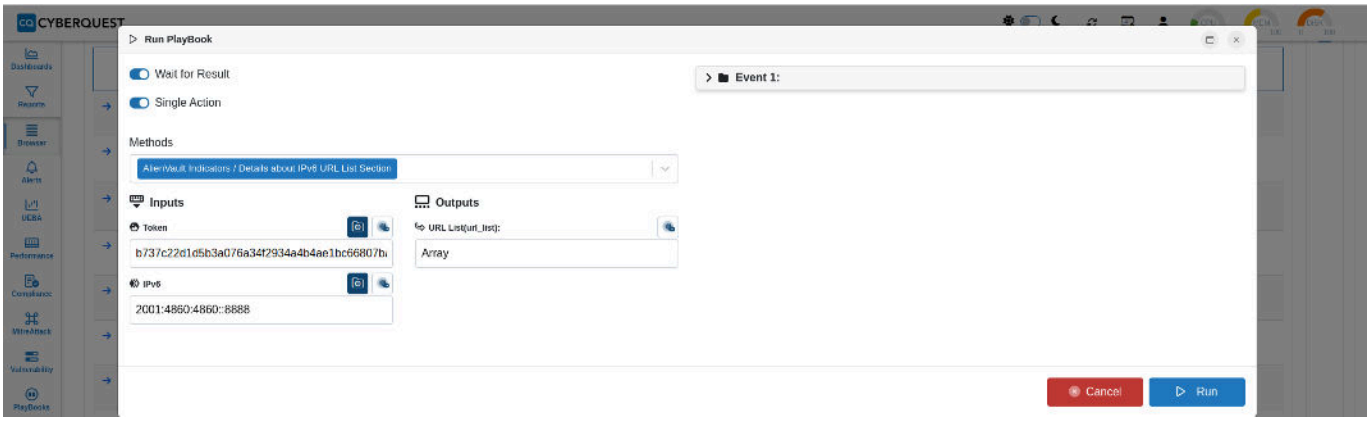


Inputs	Description
Token (is required)	To use the AlienVault API, you must have an API key
IPv6 (is required)	Retrieve details about IPv6 that will be introduced

Outputs	Description
Passive DNS(passive_dns)	A list of reports for investigated IP
Count(count)	The number of reports for the investigated IP

AlienVault Indicators/Details about IPv6 URL List Section method

Indicator page API for IPv6 Addresses.

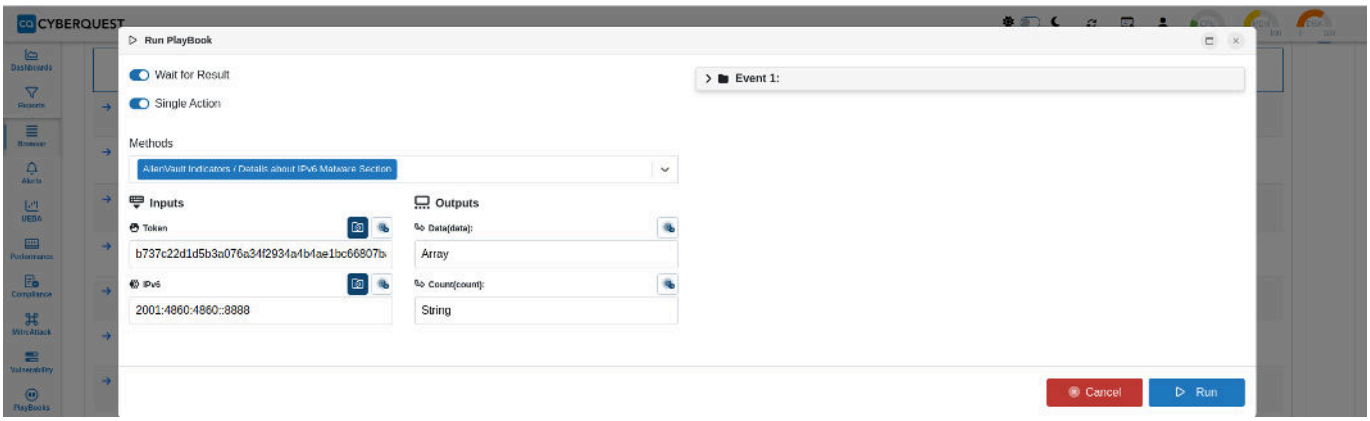


Inputs	Description
Token (is required)	To use the AlienVault API, you must have an API key
IPv6 (is required)	Retrieve details about IPv6 that will be introduced

Outputs	Description
URL List(url_list)	The reports obtained after calling the API

AlienVault Indicators/Details about IPv6 Malware Section method

Indicator page API for IPv6 Addresses.

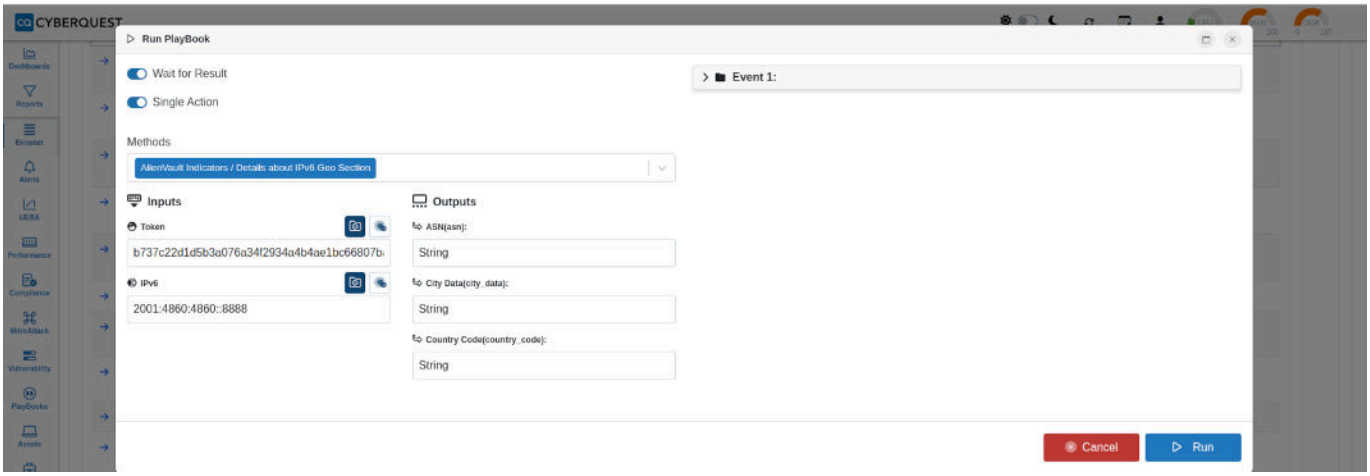


Inputs	Description
Token (is required)	To use the AlienVault API, you must have an API key
IPv6 (is required)	Retrieve details about IPv6 that will be introduced

Outputs	Description
Data (data)	The reports about the investigated IP
Count (count)	The number of reports for investigated IP

AlienVault Indicators/Details about IPv6 Geo Section method

Indicator page API for IPv6 Addresses.

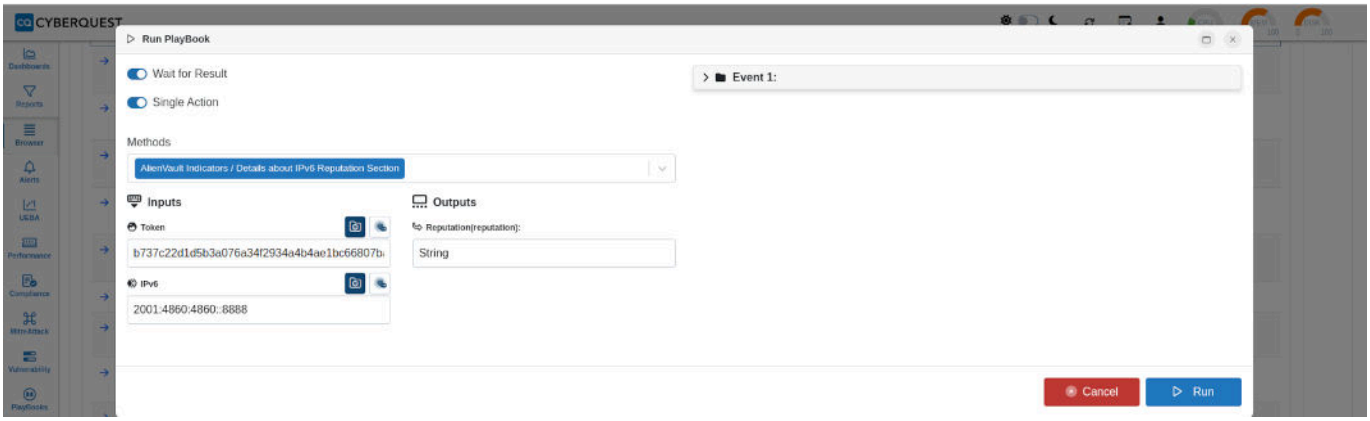


Inputs	Description
Token (is required)	To use the AlienVault API, you must have an API key
IPv6 (is required)	Retrieve details about IPv6 that will be introduced

Outputs	Description
ASN(asn)	The name of ASN
City Data(city_data)	Details about the city from where originates investigated IP
Country Code(country_code)	The country name from where originates investigated IP

AlienVault Indicators/Details about IPv6 Reputation Section method

Indicator page API for IPv6 Addresses.

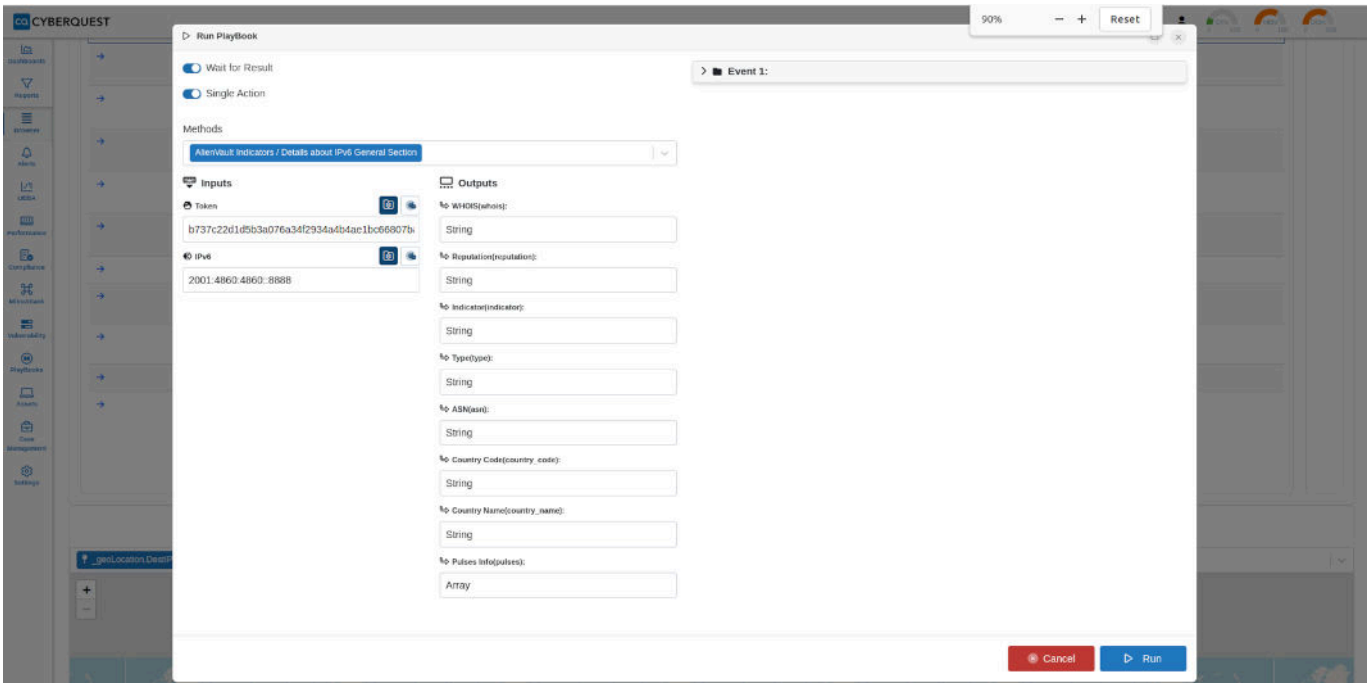


Inputs	Description
Token (is required)	To use the AlienVault API, you must have an API key
IPv6 (is required)	Retrieve details about IPv6 that will be introduced

Outputs	Description
Reputation(reputation)	This value is calculated by AlienVault, it represents the degree of trust of the investigated IP

AlienVault Indicators/Details about IPv6 General Section method

Indicator page API for IPv6 Addresses.

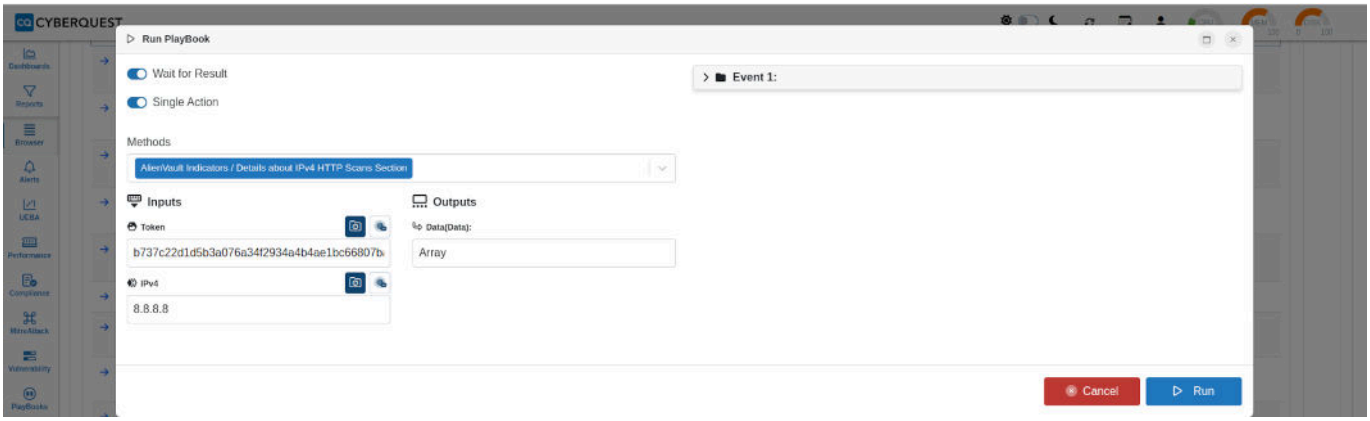


Inputs	Description
Token (is required)	To use the AlienVault API, you must have an API key
IPv6 (is required)	Retrieve details about IPv6 that will be introduced

Outputs	Description
WHOIS (whois)	An external link to gain additional WHOIS informations
Reputation (reputation)	This value is calculated by AlienVault, it represents the degree of trust of the investigated IP
Indicator (indicator)	Informations about the specific threat or security event which is investigated
Type (type)	The type of the investigated IP
ASN (asn)	The name of ASN
Country Code (country_code)	The country code from where originates investigated IP
Country Name (country_name)	The country name from where originates investigated IP
Pulses Info (pulses)	Threat summaries available in the AlienVault Open Threat Exchange (OTX)

AlienVault Indicators/Details about IPv4 HTTP Scans Section method

Indicator page API for IPv4 Addresses.

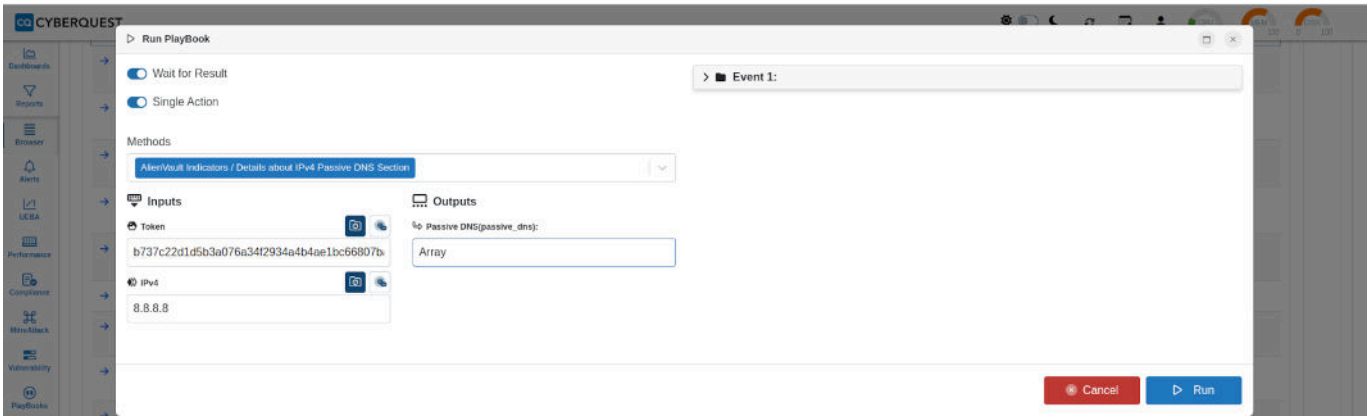


Inputs	Description
Token (is required)	To use the AlienVault API, you must have an API key
IPv4 (is required)	Retrieve details about IPv4 that will be introduced

Outputs	Description
Data(Data)	A list of reports for the intevestigated IP

AlienVault Indicators/Details about IPv4 Passive DNS Section method

Indicator page API for IPv4 Addresses.

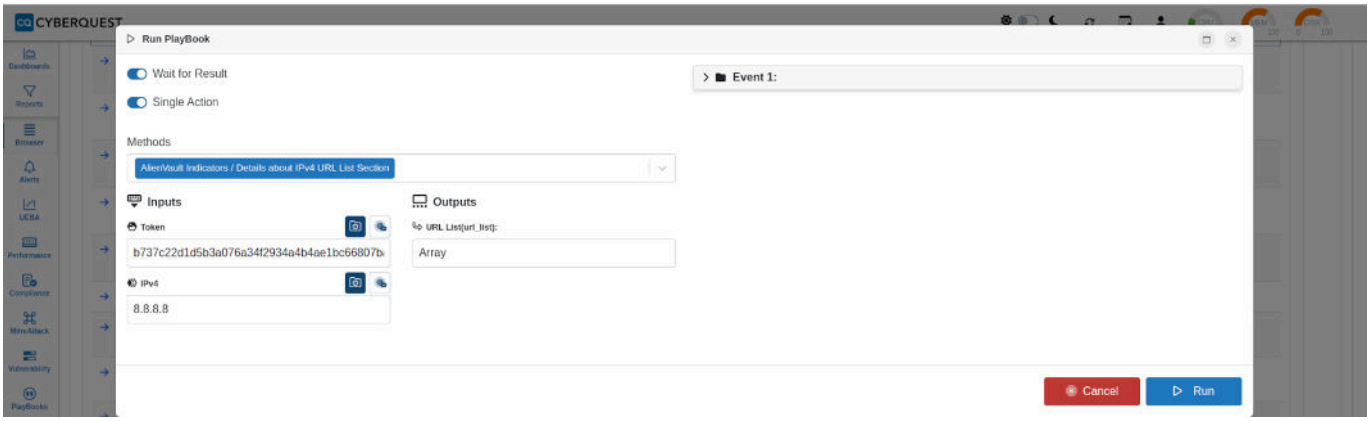


Inputs	Description
Token (is required)	To use the AlienVault API, you must have an API key
IPv4 (is required)	Retrieve details about IPv4 that will be introduced

Outputs	Description
Passive DNS(passive_dns)	A list of reports for investigated IP

AlienVault Indicators/Details about IPv4 URL List Section method

Indicator page API for IPv4 Addresses.

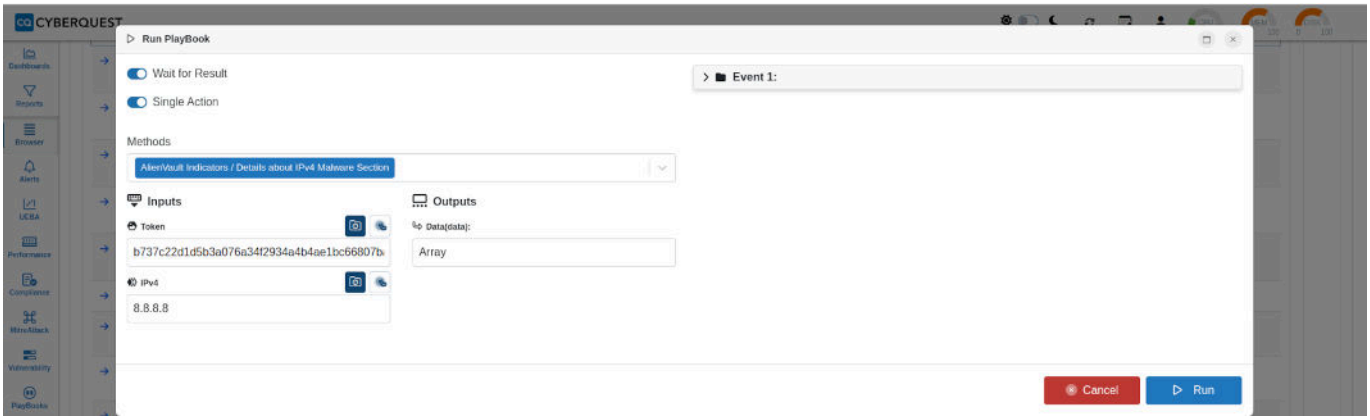


Inputs	Description
Token (is required)	To use the AlienVault API, you must have an API key
IPv4 (is required)	Retrieve details about IPv4 that will be introduced

Outputs	Description
URL List(url_list)	The reports obtained after calling the API

AlienVault Indicators/Details about IPv4 Malware Section method

Indicator page API for IPv4 Addresses.

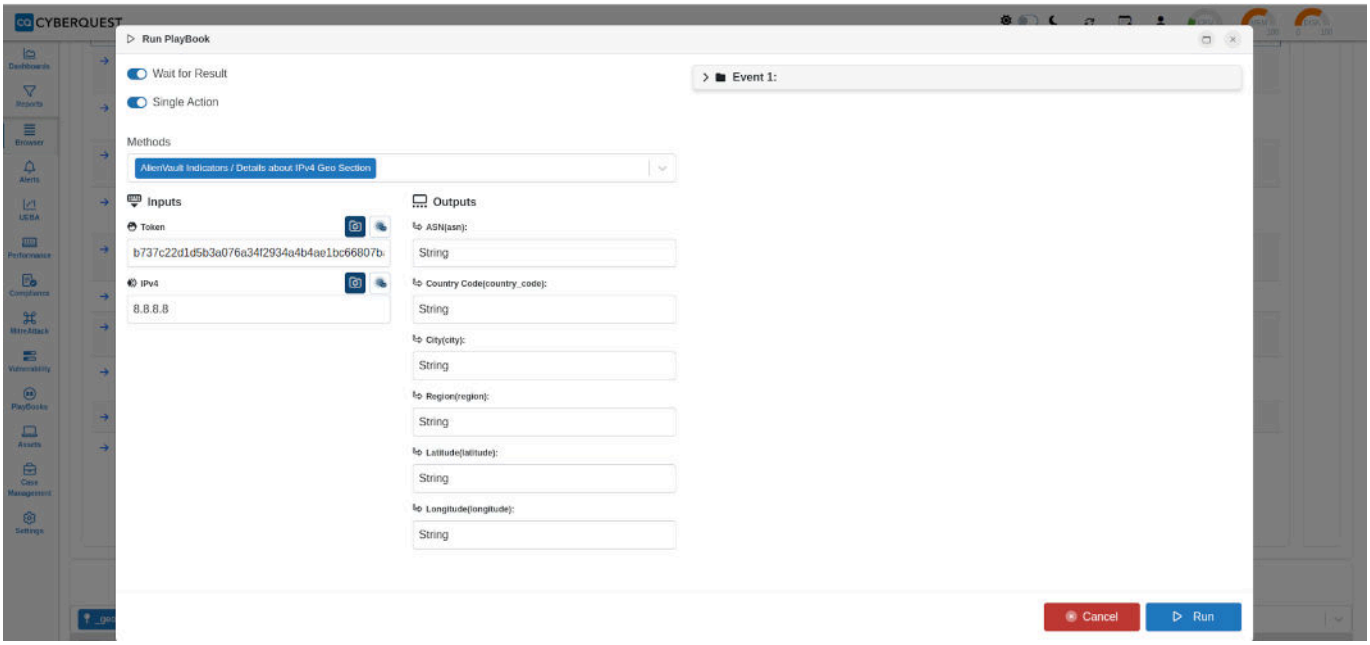


Inputs	Description
Token (is required)	To use the AlienVault API, you must have an API key
IPv4 (is required)	Retrieve details about IPv4 that will be introduced

Outputs	Description
Data(data)	The results of the API call

AlienVault Indicators/Details about IPv4 Geo Section method

Indicator page API for IPv4 Addresses.

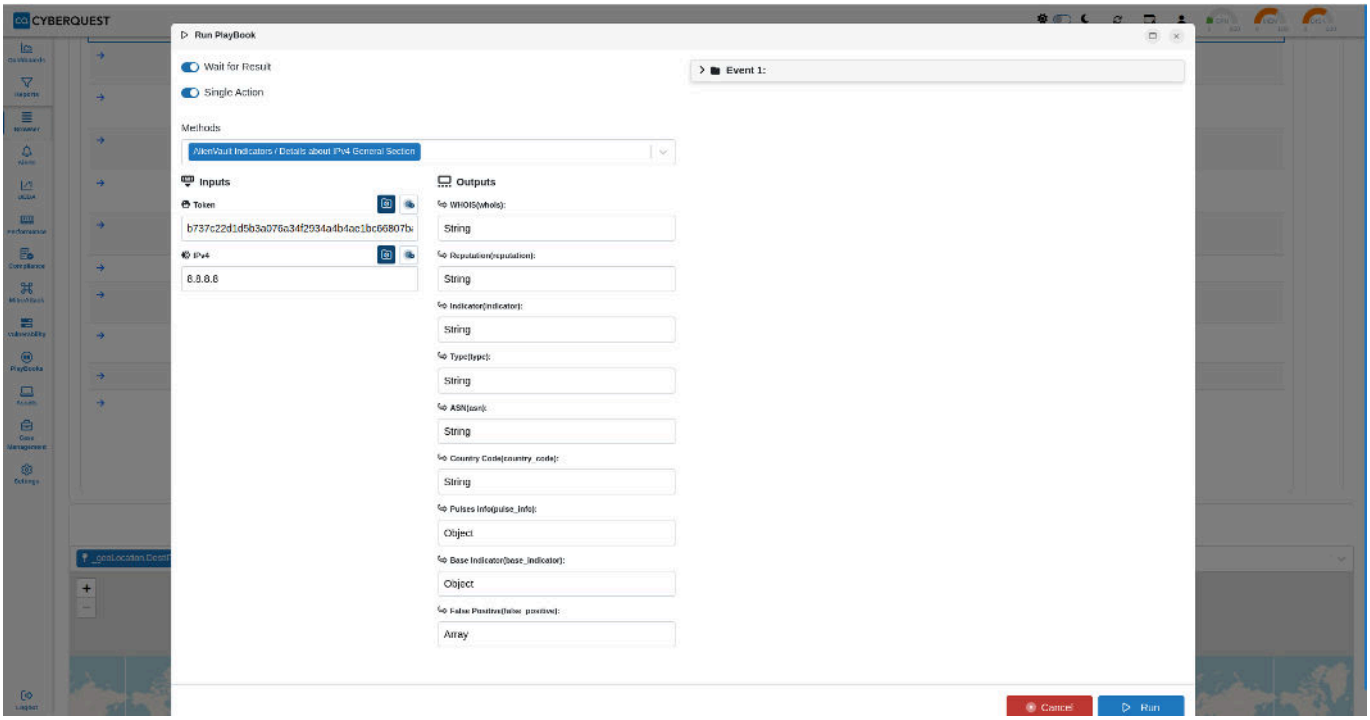


Inputs	Description
Token (is required)	To use the AlienVault API, you must have an API key
IPv4 (is required)	Retrieve details about IPv4 that will be introduced

Outputs	Description
ASN (asn)	The name of ASN
Country Code (country_code)	The country name from where originates investigated IP
City (city)	The city from where originates investigated IP
Region (region)	The region from where originates investigated IP
Latitude (latitude)	The latitude from where originates investigated IP
Longitude (longitude)	The longitude from where originates investigated IP

AlienVault Indicators/Details about IPv4 General Section method

Indicator page API for IPv4 Addresses.

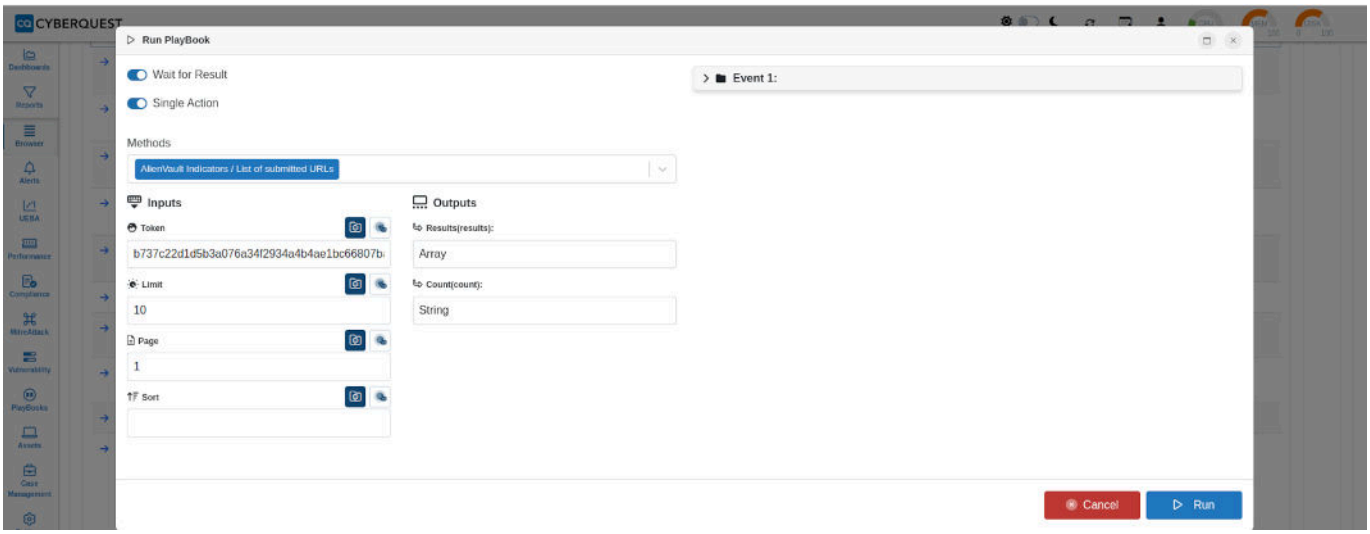


Inputs	Description
Token (is required)	To use the AlienVault API, you must have an API key
IPv4 (is required)	Retrieve details about IPv4 that will be introduced

Outputs	Description
WHOIS (whois)	An external link to gain additional WHOIS informations
Reputation (reputation)	This value is calculated by AlienVault, it represents the degree of trust of the investigated IP
Indicator (indicator)	Informations about the specific threat or security event which is investigated
Type (type)	The type of the investigated IP
ASN (asn)	The name of ASN
Country Code (country_code)	The country name from where originates investigated IP
Pulses info (pulse_info)	Threat summaries available in the AlienVault Open Threat Exchange (OTX).
Base Indicator (base_indicator)	Essential information about the specific threat or security event which is investigated
False Positive (false_positive)	An Array which includes the false positives detected

AlienVault Indicators/List of submitted URLs method

Returns a list of all submitted URLs, along with the status of the submission.

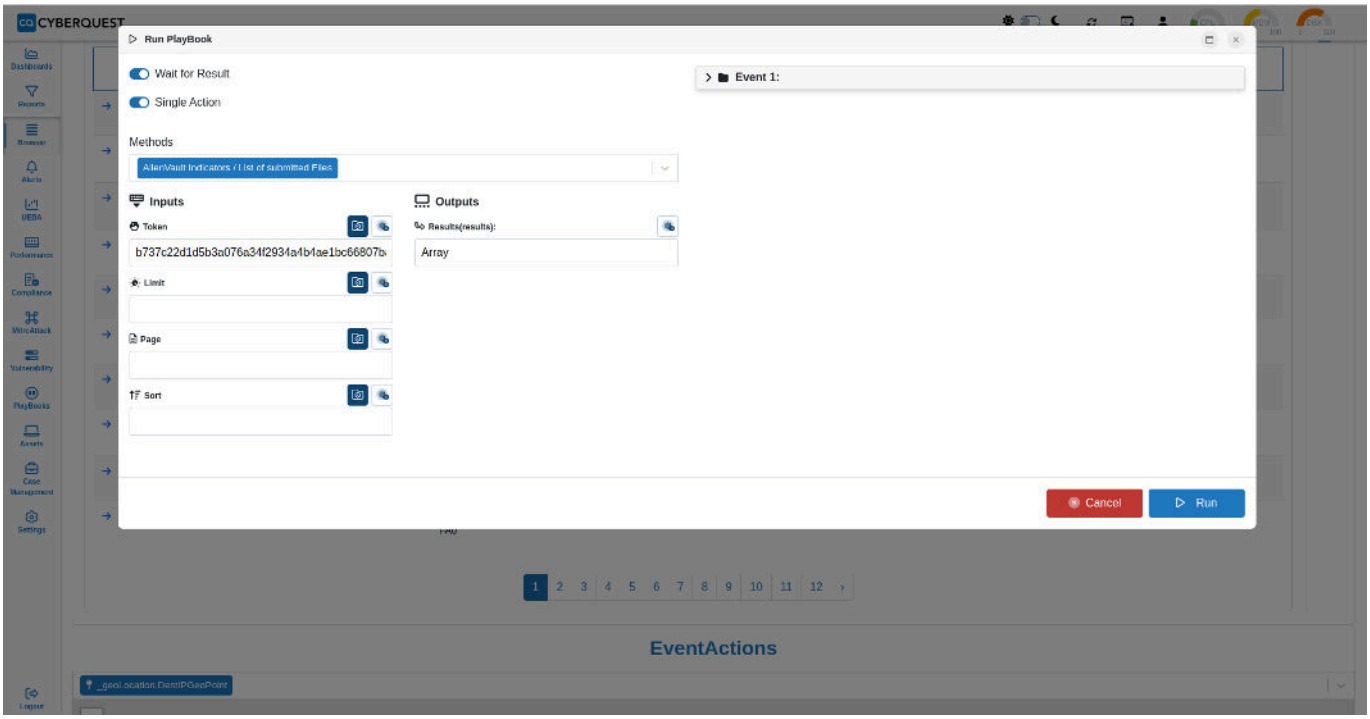


Inputs	Description
Token (is required)	To use the AlienVault API, you must have an API key
Limit	Number of results to include per page
Page	Which page of results is desired
Sort	Order by one of these fields: add_date,url,complete_date

Outputs	Description
Results(results)	A list with subbmited URLs
Count(count)	The number of submitted URLs for investigation

AlienVault Indicators/List of submitted Files method

Returns a list of all submitted files, along with the status of the submission.



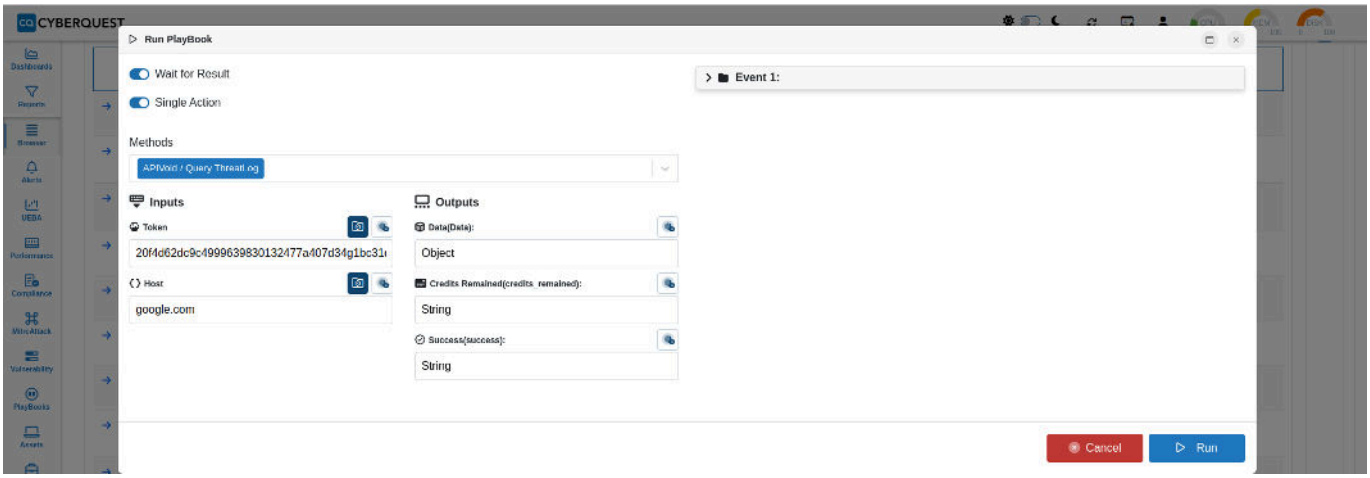
Inputs	Description
Token (is required)	To use the AlienVault API, you must have an API key
Limit	Number of results to include per page
Page	Which page of results is desired
Sort	Order by one of these fields: add_date,sha256,complete_date

Outputs	Description
Result(result)	The result of analysis

APIVoid

APIVoid/Query ThreatLog method

This API lets you query ThreatLog.com database of malicious domains.

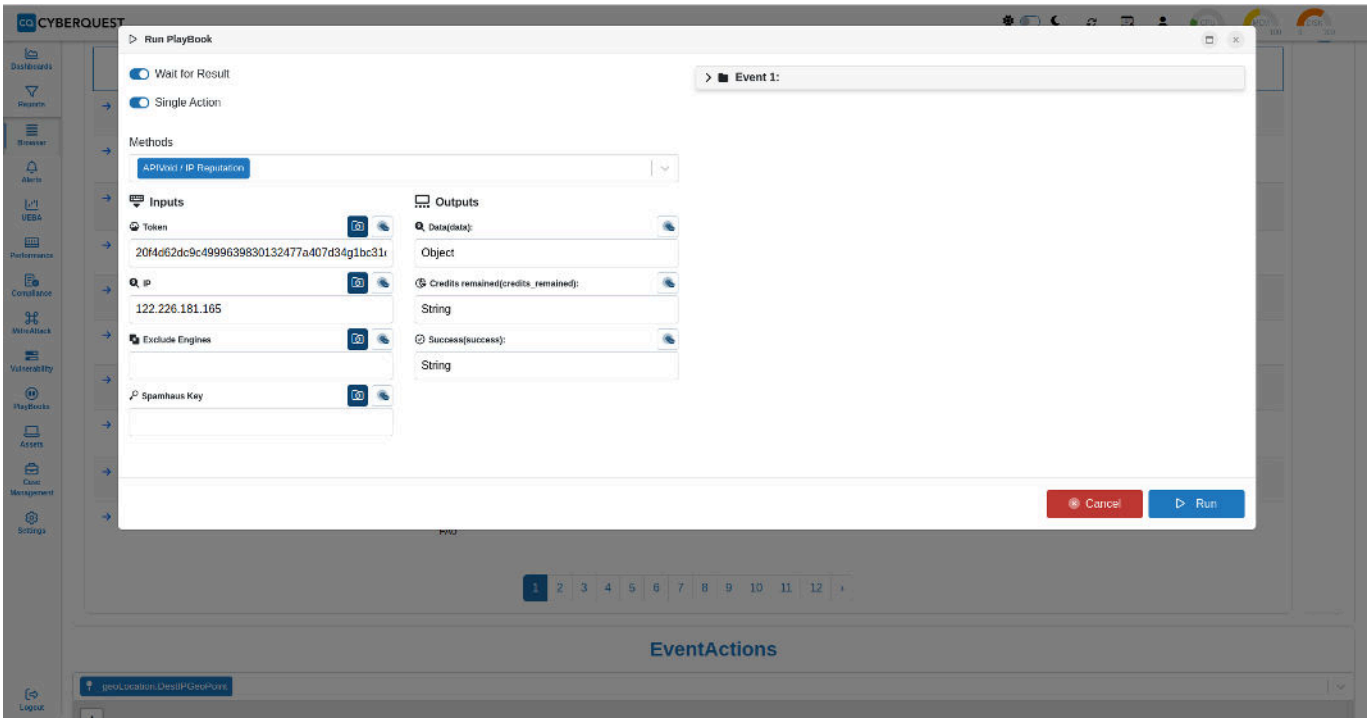


Inputs	Description
Token (is required)	Your APIVoids API key
Host (is required)	Host to submit

Outputs	Description
Data (Data)	The result of the API call
Credits Remained (credits_remained)	The number of the remained credits
Success (success)	True if the API call is successfully executed, false if not

APIVoid/IP Reputation method

This API lets you check the reputation and geolocation of an IPv4 address.Additionally the API also detects public proxy, web proxy, Tor and VPN IP addresses.

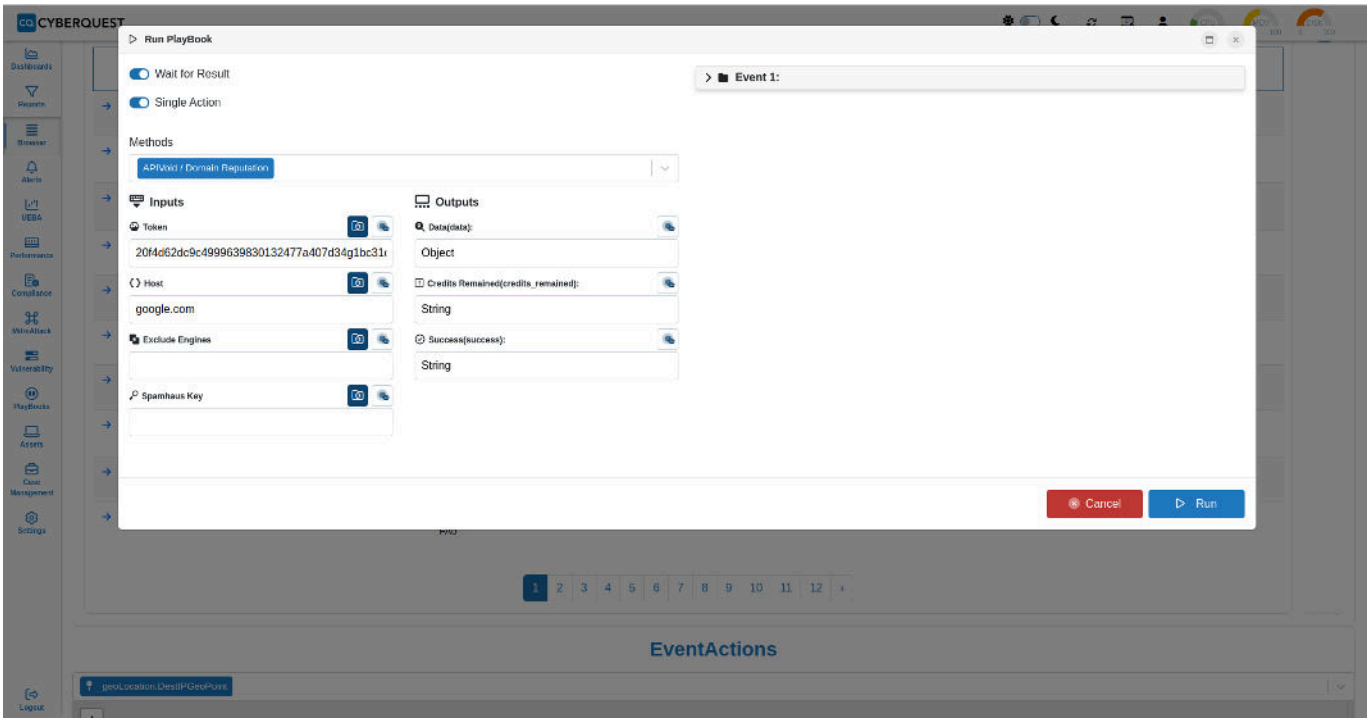


Inputs	Description
Token (is required)	Your APIVoids API key
IP (is required)	IPv4 address to submit
Exclude Engines	List of comma-separated engines to exclude
Spamhaus Key	Your Spamhaus ZEN DQS key, this will enable Spamhaus engine

Outputs	Description
Data (data)	The result of the API call
Credits remained (credits_remained)	The number of the remained credits
Success (success)	True if the API call is successfully executed, false if not

APIVoid/Domain Reputation method

This API lets you check if a domain name is blacklisted by trusted sources.

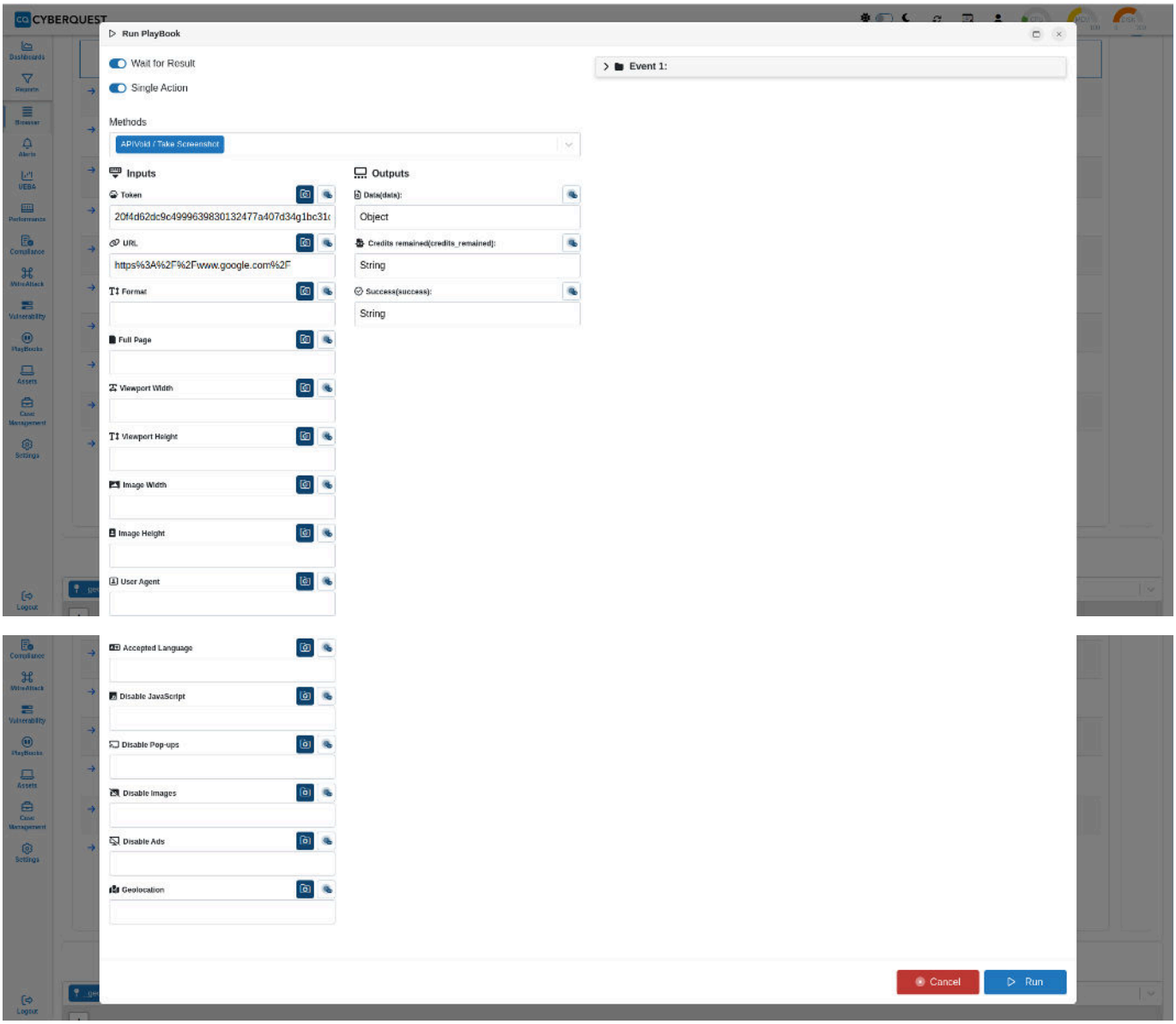


Inputs	Description
Token (is required)	Your APIVoids API key
Host (is required)	Host to submit
Exclude Engines	List of comma-separated engines to exclude
Spamhaus Key	Your Spamhaus DBL DQS key, this will enable Spamhaus engine

Outputs	Description
Data (data)	The result of the API call
Credits Remained (credits_remained)	The number of the remained credits
Success (success)	True if the API call is successfully executed, false if not

APIVoid/Take Screenshot method

This API lets you take high-quality screenshots of any web page and URL.

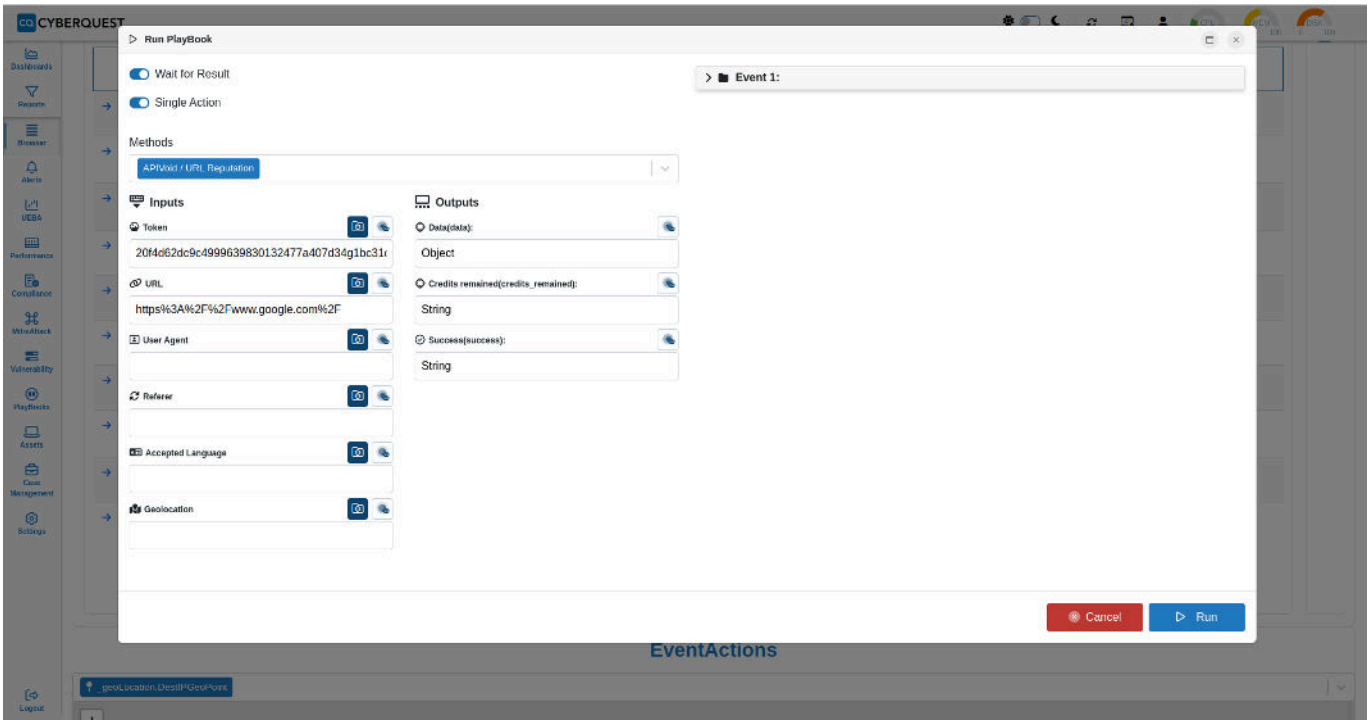

CYBERQUEST
Run PlayBook
Wait for Result
Single Action
Methods
APIVoid / Take Screenshot
Inputs
Token
20f4d62dc9c4999639830132477a407d34g1bc31c
URL
https%3A%2F%2Fwww.google.com%2F
Format
Full Page
Viewport Width
Viewport Height
Image Width
Image Height
User Agent
Outputs
Data(data):
Object
Credits remained(credits_remained):
String
Success(success):
String
Event 1:
Accepted Language
Disable JavaScript
Disable Pop-ups
Disable Images
Disable Ads
Geolocation
Cancel
Run

Inputs	Description
Token (is required)	Your APIVoids API key
URL (is required)	URL to submit, must be encoded
Format	Image format, can be png or jpg
Full Page	Lets you take a full page screenshot
Viewport Width	Lets you change browser viewport width in pixels
Viewport Height	Lets you change browser viewport height in pixels
Image Width	Lets you change the thumbnail image width in pixels
Image Height	Lets you change the thumbnail image height in pixels
User Agent	Lets you change the browser user agent string, must be encoded
Accepted Language	Lets you change the accept language HTTP header, format is like en or en-US
Disable JavaScript	Lets you disable JavaScript
Disable Pop-ups	Lets you disable alerts, prompts and confirmation dialogs
Disable Images	Lets you disable loading of images
Disable Ads	Lets you disable advertisements
Geolocation	Change geolocation

Outputs	Description
Data (data)	The result of the API call
Credits remained (credits_remained)	The number of the remained credits
Success (success)	True if the API call is successfully executed, false if not

APIVoid/URL Reputation method

This API can help you identify potentially unsafe and phishing URLs.

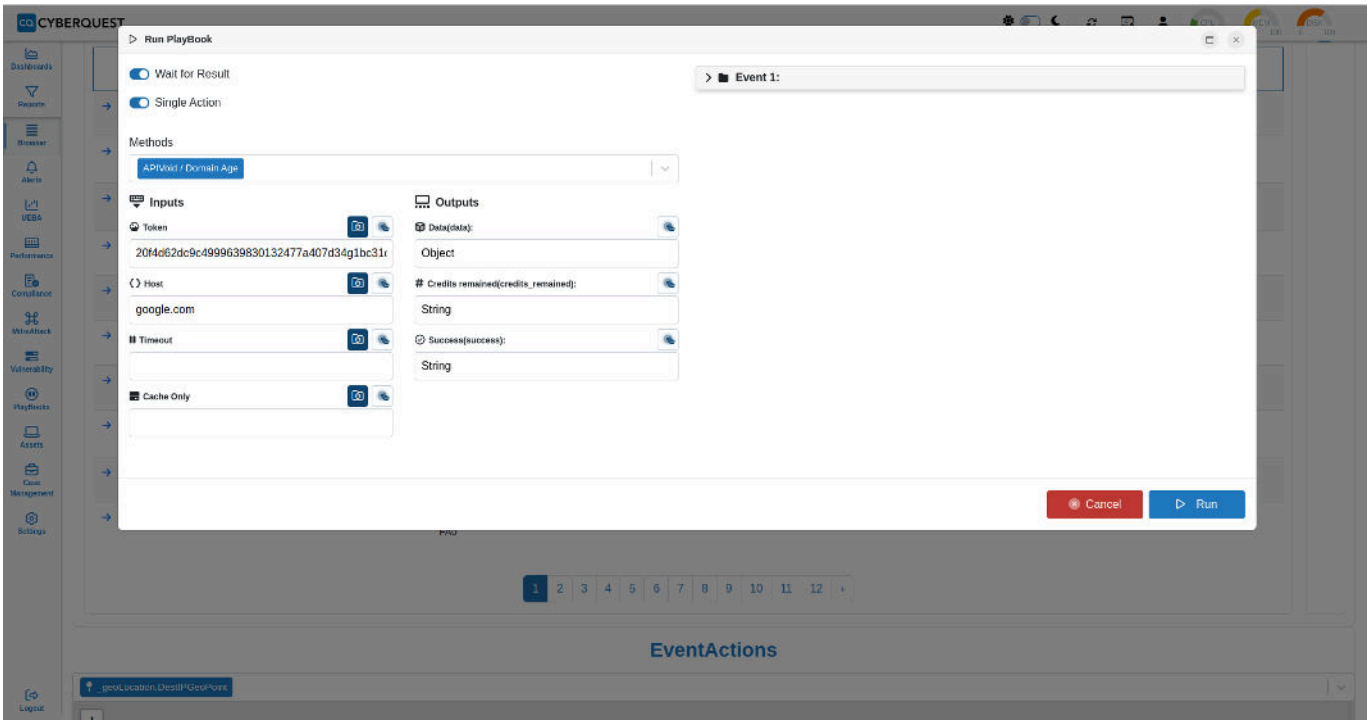


Inputs	Description
Token (is required)	Your APIVoids API key
URL (is required)	URL to submit, must be encoded
User Agent	Lets you change the browser user agent string, must be encoded
Referer	Lets you change the referer URL
Accepted Language	Lets you change the accept language HTTP header, format is like en or en-US
Geolocation	Change geolocation

Outputs	Description
Data (data)	The result of the API call
Credits remained (credits_remained)	The number of the remained credits
Success (success)	True if the API call is successfully executed, false if not

APIVoid/Domain Age method

This API lets you get domain registration date and domain age in days.

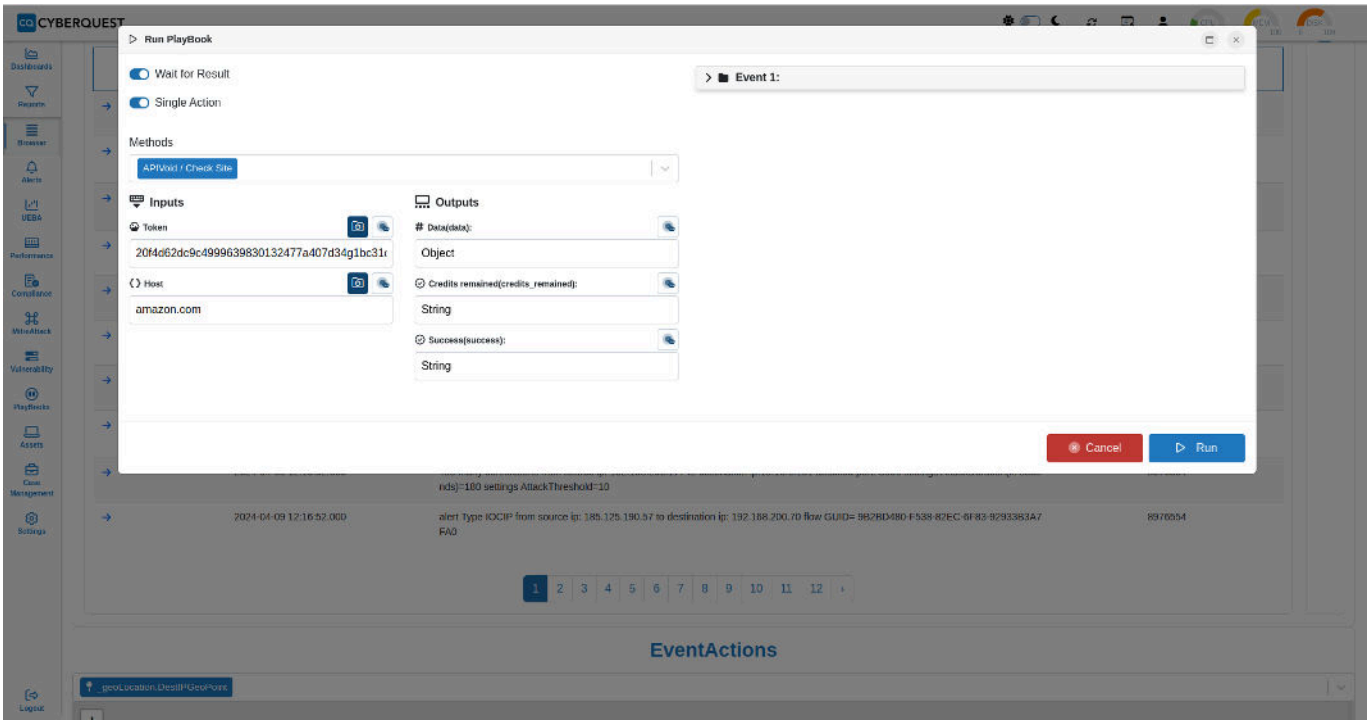


Inputs	Description
Token (is required)	Your APIVoids API key
Host (is required)	Host to submit
Timeout	Set a custom timeout in seconds, can be from 5 to 30 seconds
Cache Only	Get data only from cache (if present) for faster response

Outputs	Description
Data (data)	The result of the API call
Credits remained (credits_remained)	The number of the remained credits
Success (success)	True if the API call is successfully executed, false if not

APIVoid/Check Site method

This API provides you important details about a website to check if it is legit.

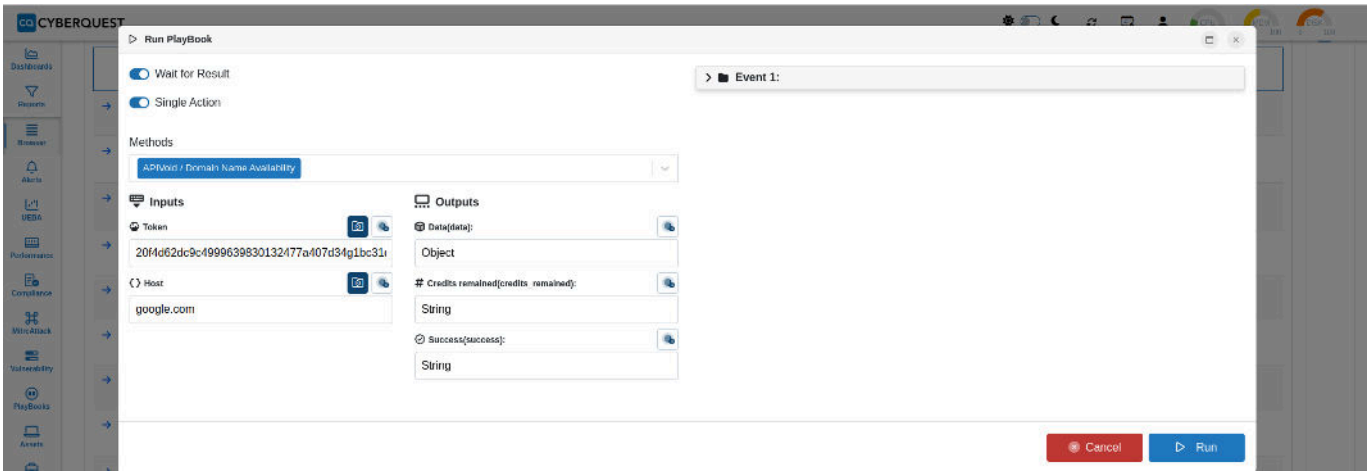


Inputs	Description
Token (is required)	Your APIVoids API key
Host (is required)	Host to submit

Outputs	Description
Data (data)	The result of the API call
Credits remained (credits_remained)	The number of the remained credits
Success (success)	True if the API call is successfully executed, false if not

APIVoid/Domain Name Availability method

This API lets you check if a domain name is parked/for sale.

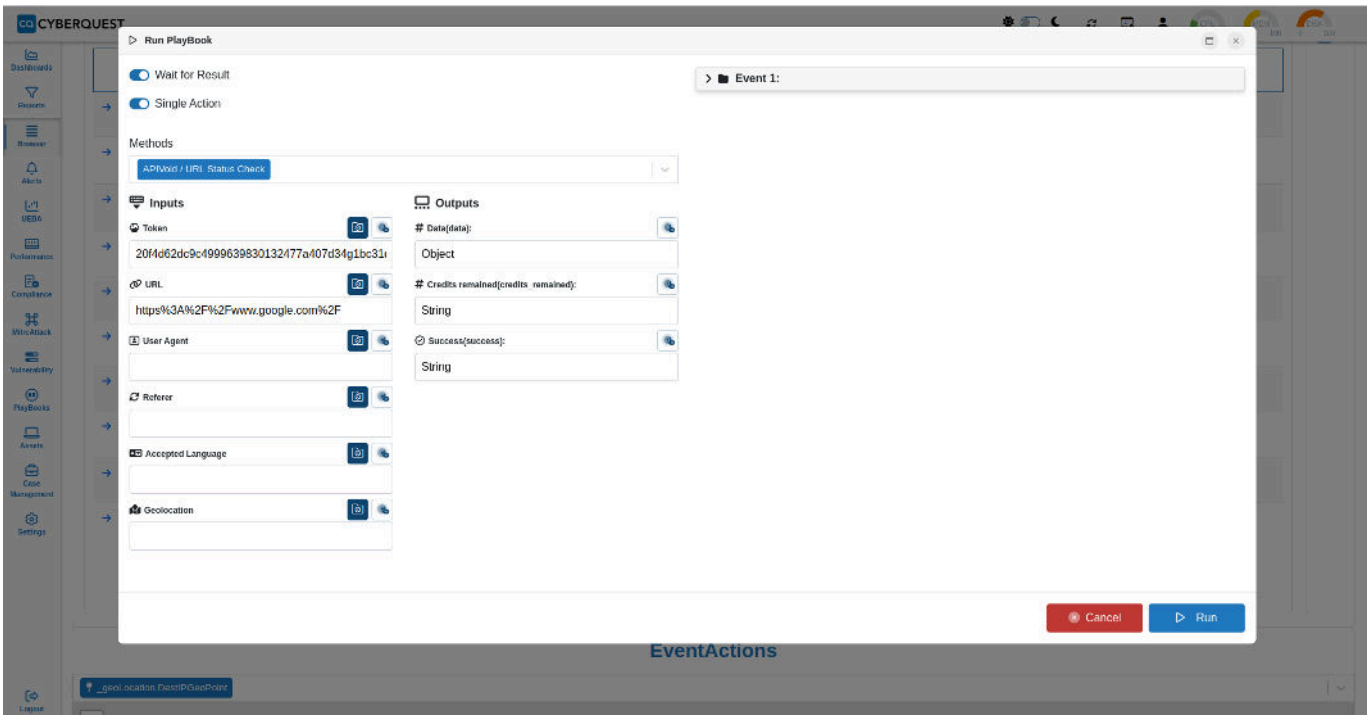


Inputs	Description
Token (is required)	Your APIVoids API key
Host (is required)	Host to submit

Outputs	Description
Data (data)	The result of the API call
Credits remained (credits_remained)	The number of the remained credits
Success (success)	True if the API call is successfully executed, false if not

APIVoid/URL Status Check method

This API lets you check if an URL is online or offline (down or not accessible).

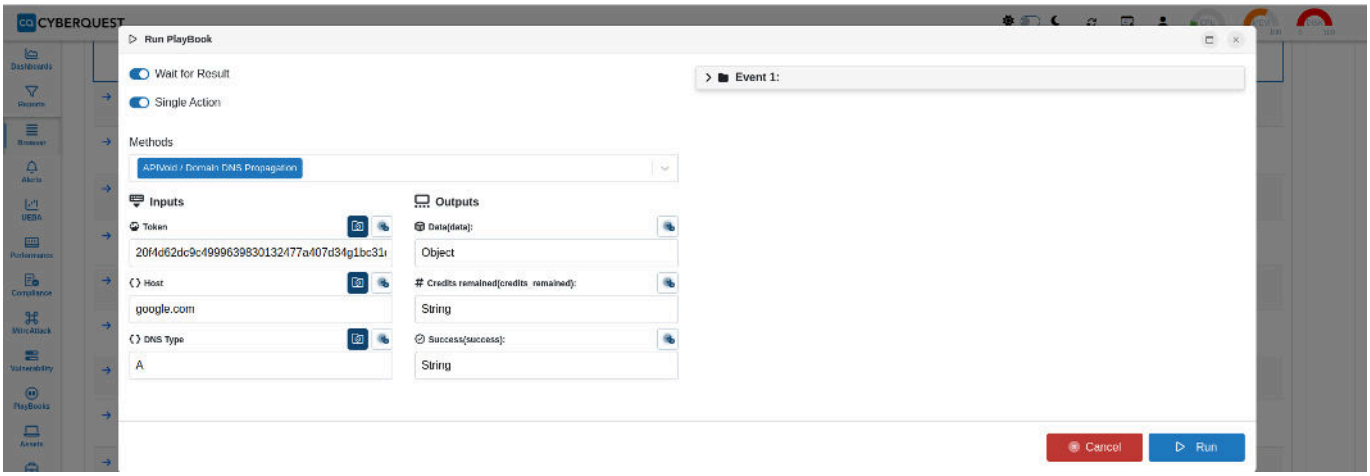


Inputs	Description
Token (is required)	Your APIVoids API key
URL (is required)	Host to submitURL to submit, must be encoded
User Agent	Lets you change the browser user agent string, must be encoded
Referer	Lets you change the referer URL
Accepted Language	Lets you change the accept language HTTP header, format is like en or en-US
Geolocation	Change geolocation

Outputs	Description
Data (data)	The result of the API call
Credits remained (credits_remained)	The number of the remained credits
Success (success)	True if the API call is successfully executed, false if not

APIVoid/Domain DNS Propagation method

This API lets you check if DNS records of a domain have propagated globally.

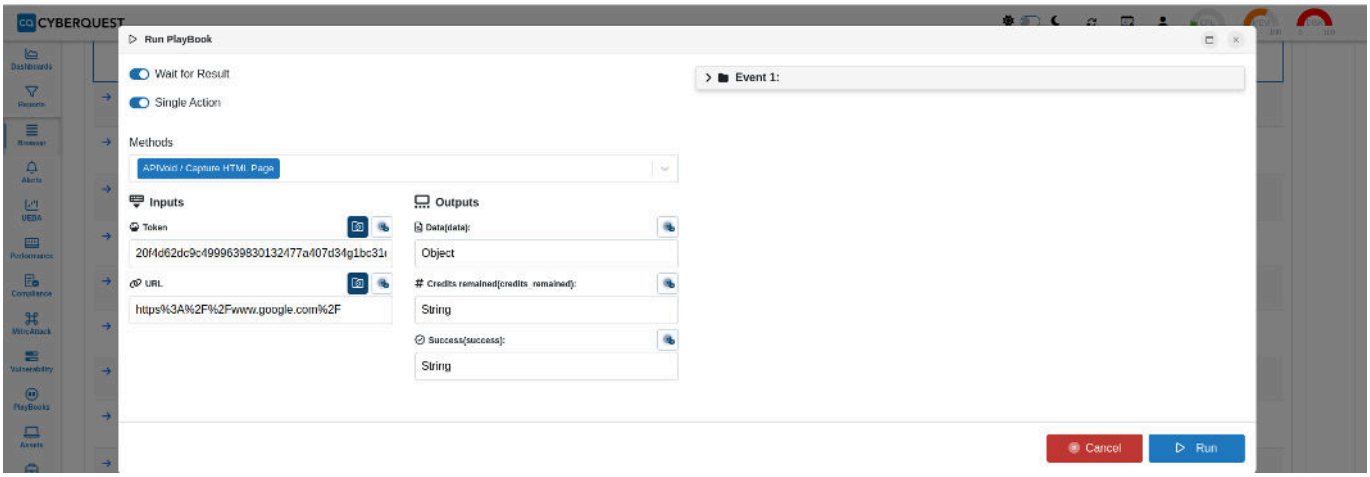


Inputs	Description
Token (is required)	Your APIVoids API key
Host (is required)	Host to submit
DNS Type (is required)	DNS type

Outputs	Description
Data (data)	The result of the API call
Credits remained (credits_remained)	The number of the remained credits
Success (success)	True if the API call is successfully executed, false if notOutputs

APIVoid/Capture HTML Page method

This API lets you capture the HTML page source after JavaScript has been executed.

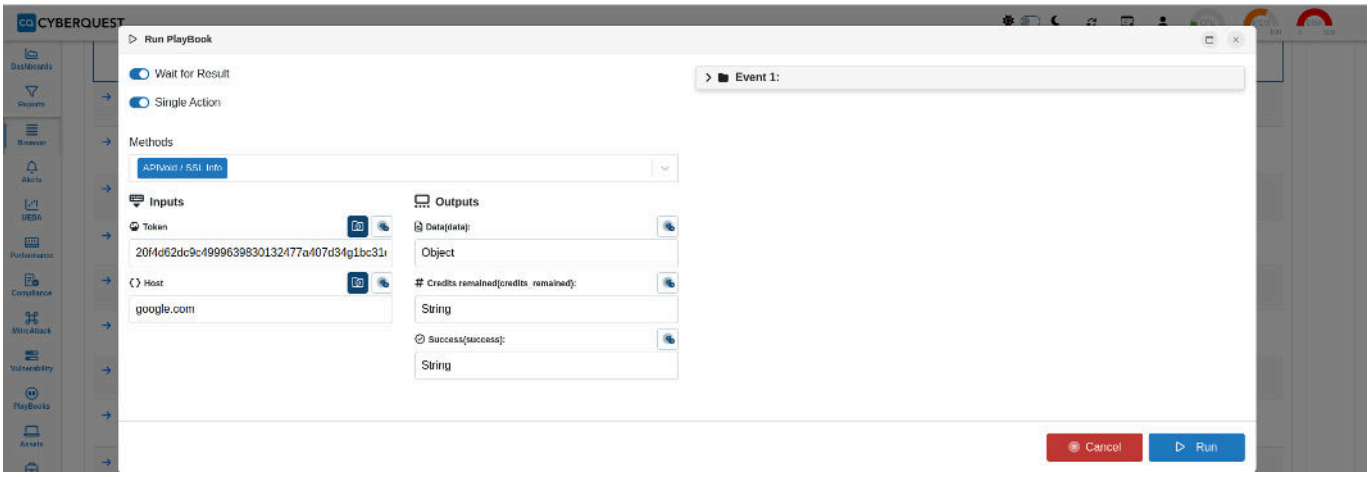


Inputs	Description
Token (is required)	Your APIVoids API key
URL (is required)	URL to submit, must be encoded

Outputs	Description
Data (data)	The result of the API call
Credits remained (credits_remained)	The number of the remained credits
Success (success)	True if the API call is successfully executed, false if not

APIVoid/SSL Info method

This API provides you details about a websites SSL certificate.

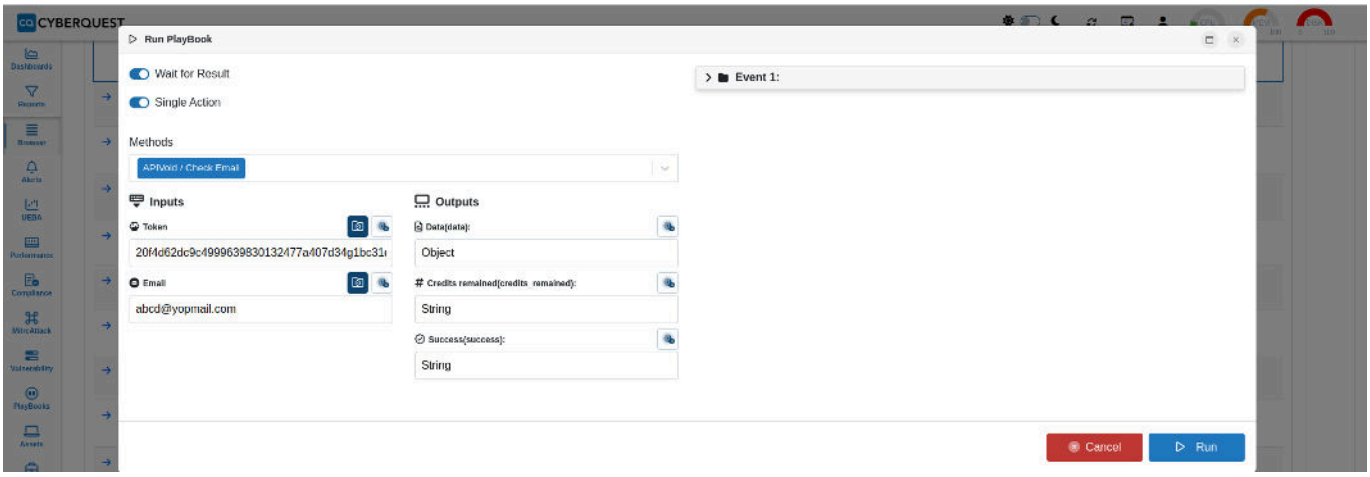


Inputs	Description
Token (is required)	Your APIVoids API key
Host (is required)	Host to submit, i.e google.com

Outputs	Description
Data (data)	The result of the API call
Credits remained (credits_remained)	The number of the remained credits
Success (success)	True if the API call is successfully executed, false if not

APIVoid/Check Email method

This API provides you useful information about an email address.

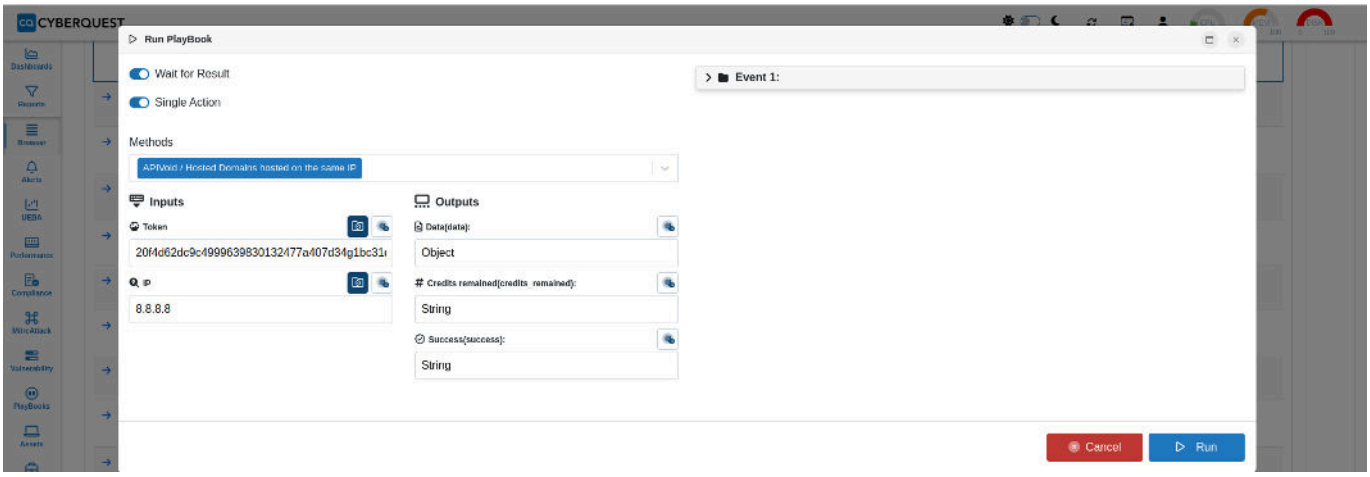


Inputs	Description
Token (is required)	Your APIVoids API key
Email (is required)	Email to submit

Outputs	Description
Data (data)	The result of the API call
Credits remained (credits_remained)	The number of the remained credits
Success (success)	True if the API call is successfully executed, false if not

APIVoid/Hosted Domains hosted on the same IP method

This API lets you find a list of domains hosted on the same IPv4 address.

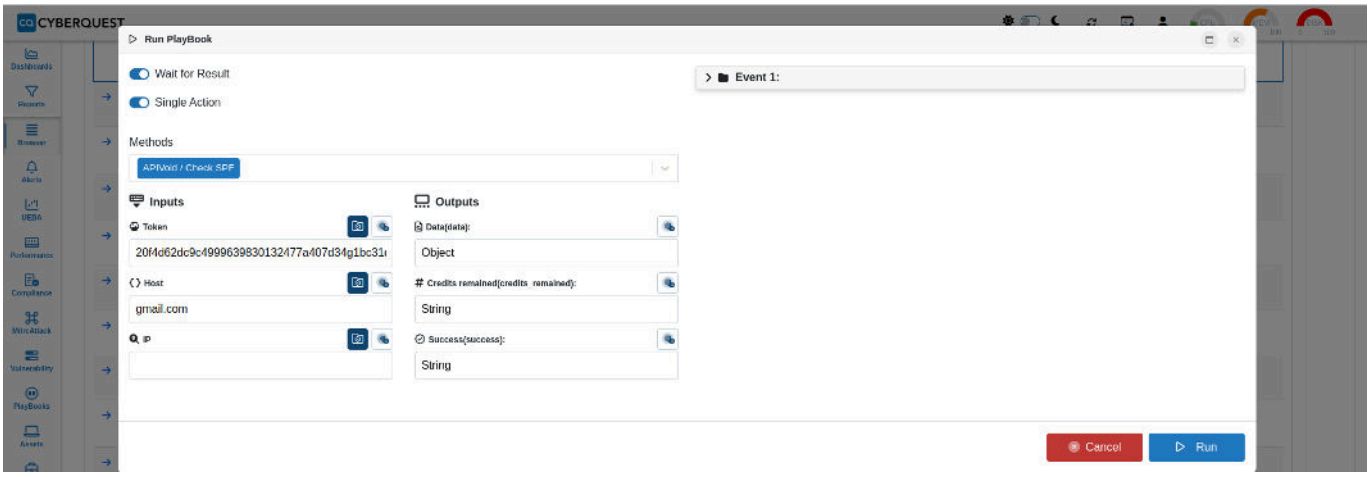


Inputs	Description
Token (is required)	Your APIVoids API key
IP (is required)	IPv4 address to submit

Data (data)	The result of the API call
Credits remained (credits_remained)	The number of the remained credits
Outputs	Description
Success (success)	True if the API call is successfully executed, false if not

APIVoid/Check SPF method

This API lets you check and validate SPF record of any domain.

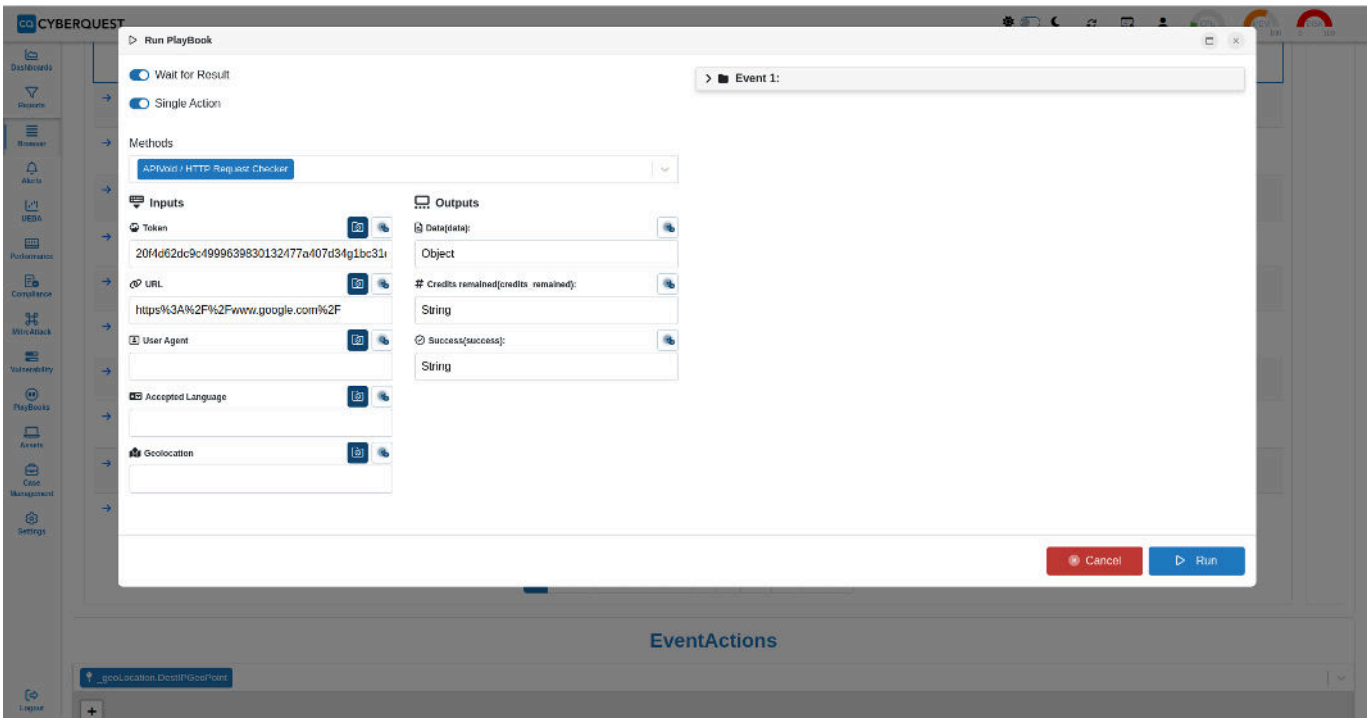


Inputs	Description
Token (is required)	Your APIVoids API key
Host (is required)	Host to submit
IP	IPv4 or IPv6 address you want to check if it is authorized to send emails

Outputs	Description
Data (data)	The result of the API call
Credits remained (credits_remained)	The number of the remained credits
Success (success)	True if the API call is successfully executed, false if not

APIVoid/HTTP Request Checker method

This API lets you check HTTP requests made by an URL or a website.

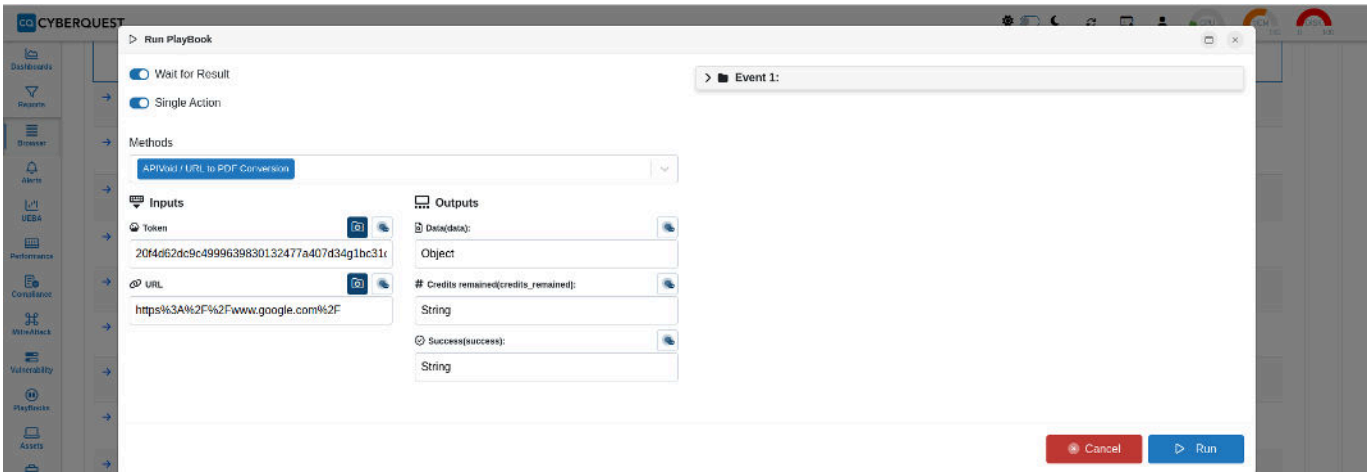


Inputs	Description
Token (is required)	Your APIVoids API key
URL (is required)	URL to submit, must be encoded
User Agent	Lets you change the browser user agent string, must be encoded
Accepted Language	Lets you change the accept language HTTP header, format is like en or en-US
Geolocation	Change geolocation

Outputs	Description
Data (data)	The result of the API call
Credits remained (credits_remained)	The number of the remained credits
Success (success)	True if the API call is successfully executed, false if not

APIVoid/URL to PDF Conversion method

This API lets you convert an URL into a high-quality PDF document.

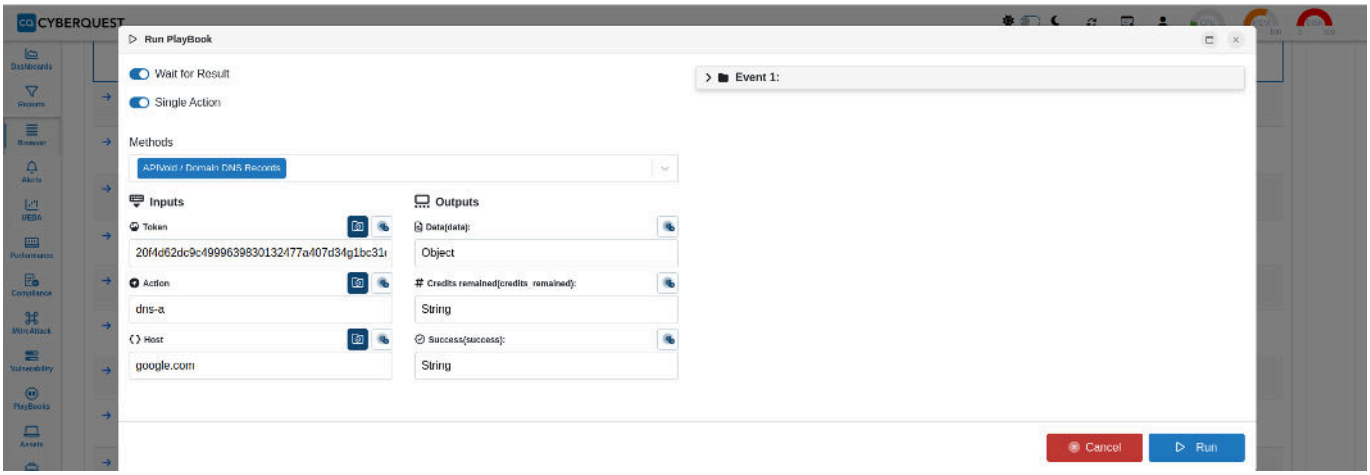


Inputs	Description
Token (is required)	Your APIVoids API key
URL (is required)	URL to submit, must be encoded

Outputs	Description
Data (data)	The result of the API call
Credits remained (credits_remained)	The number of the remained credits
Success (success)	True if the API call is successfully executed, false if not

APIVoid/Domain DNS Records method

This API lets you easily get DNS records of domain names.



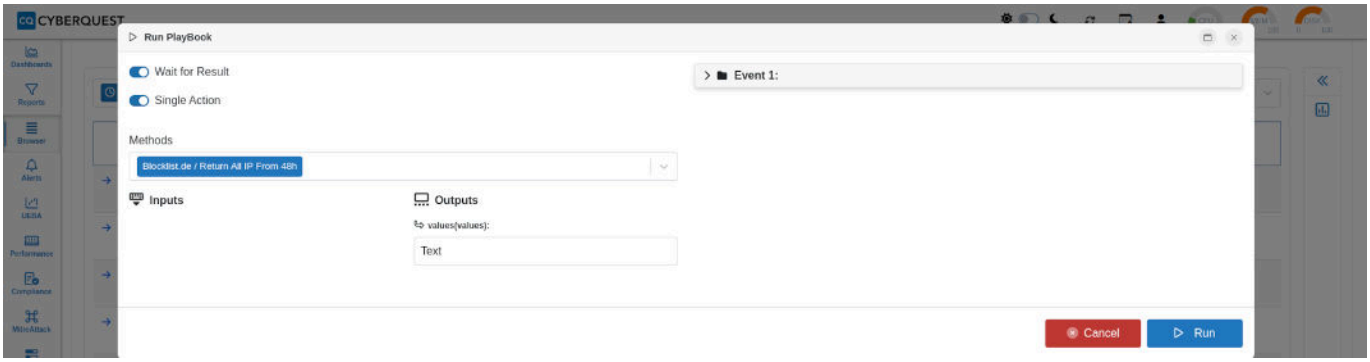
Inputs	Description
Token (is required)	Your APIVoids API key
Action (is required)	DNS lookup type, can be dns-a, dns-aaaa, dns-mx, dns-ns, dns-dmarc, dns-ptr, dns-txt, dns-any, dns-cname, dns-soa, dns-srv, dns-caa
Host (is required)	Host to submit

Outputs	Description
Data (data)	The result of the API call
Credits remained (credits_remained)	The number of the remained credits
Success (success)	True if the API call is successfully executed, false if not

Blocklist.de

Blocklist.de/Return all IP from 48h method

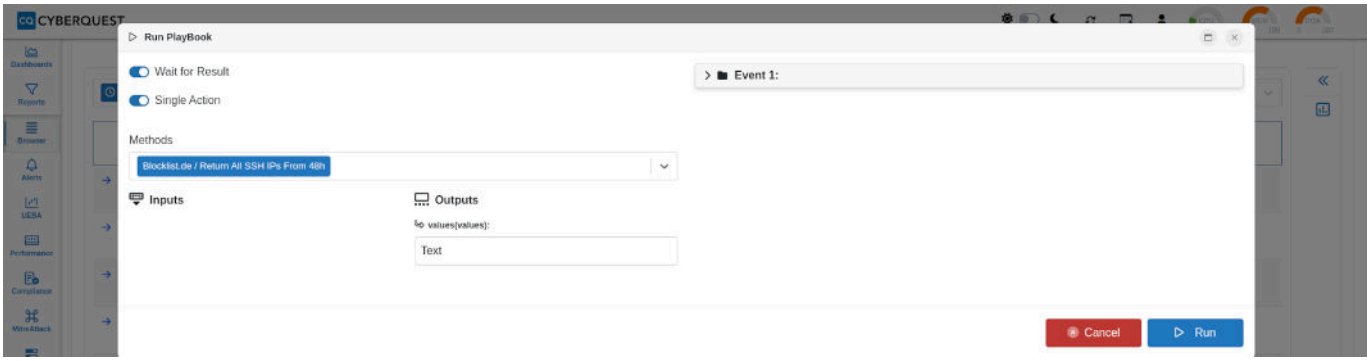
All IP addresses that have attacked one of our customers/servers in the last 48 hours.



Outputs	Description
values(values)	The results of the API call

Blocklist.de/Return All SSH IPs from 48h method

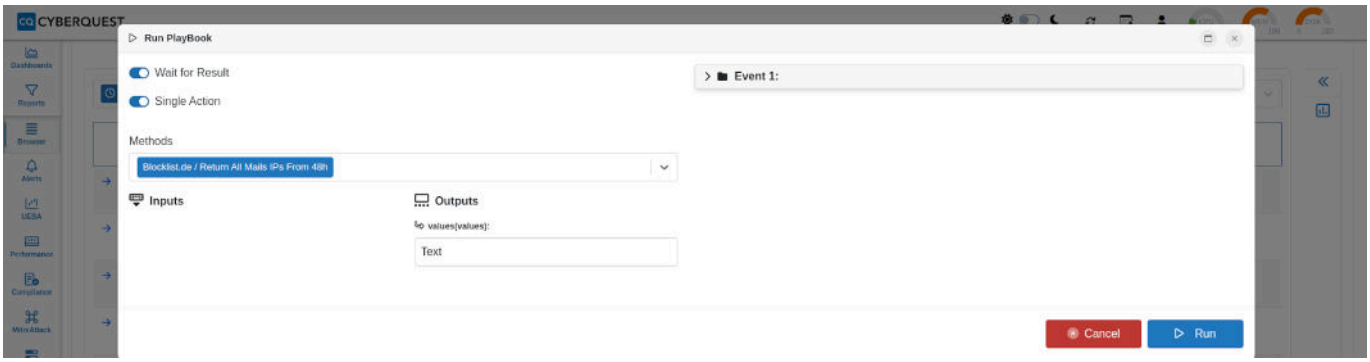
All IP addresses that have attacked one of our customers/servers in the last 48 hours.



Outputs	Description
values(values)	The results of the API call

Blocklist.de/Return All Mails IPs from 48h method

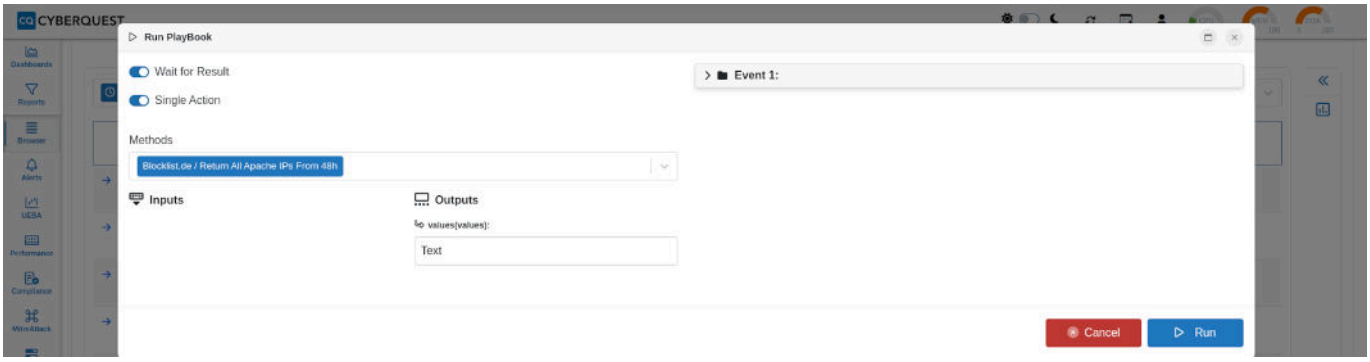
All IP addresses that have attacked one of our customers/servers in the last 48 hours.



Outputs	Description
values(values)	The results of the API call

Blocklist.de/Return All Apache IPs from 48h method

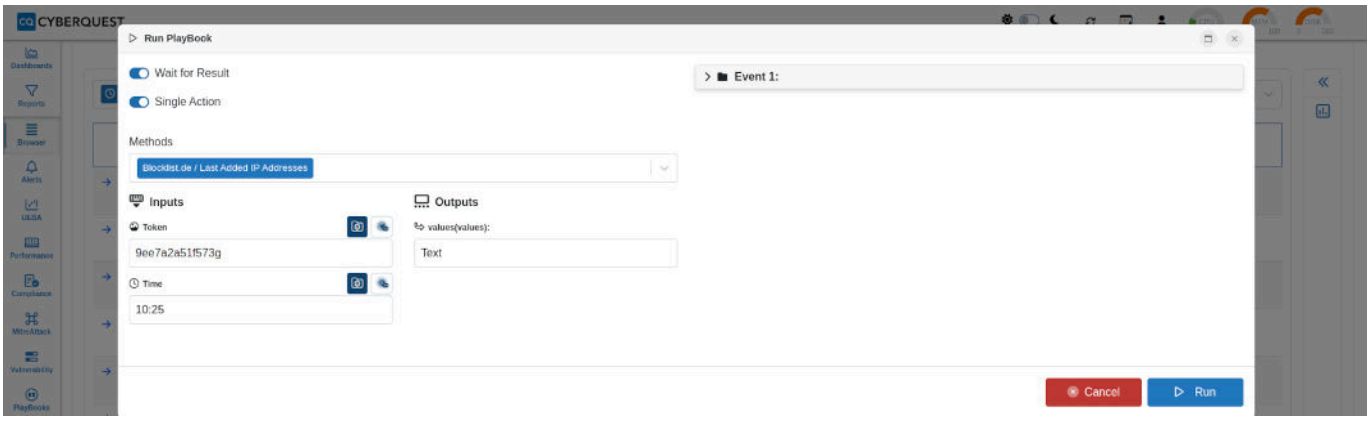
All IP addresses that have attacked one of our customers/servers in the last 48 hours.



Outputs	Description
values(values)	The results of the API call

Blocklist.de/Last Added IP Addresses method

Get only the last added IP Addresses.

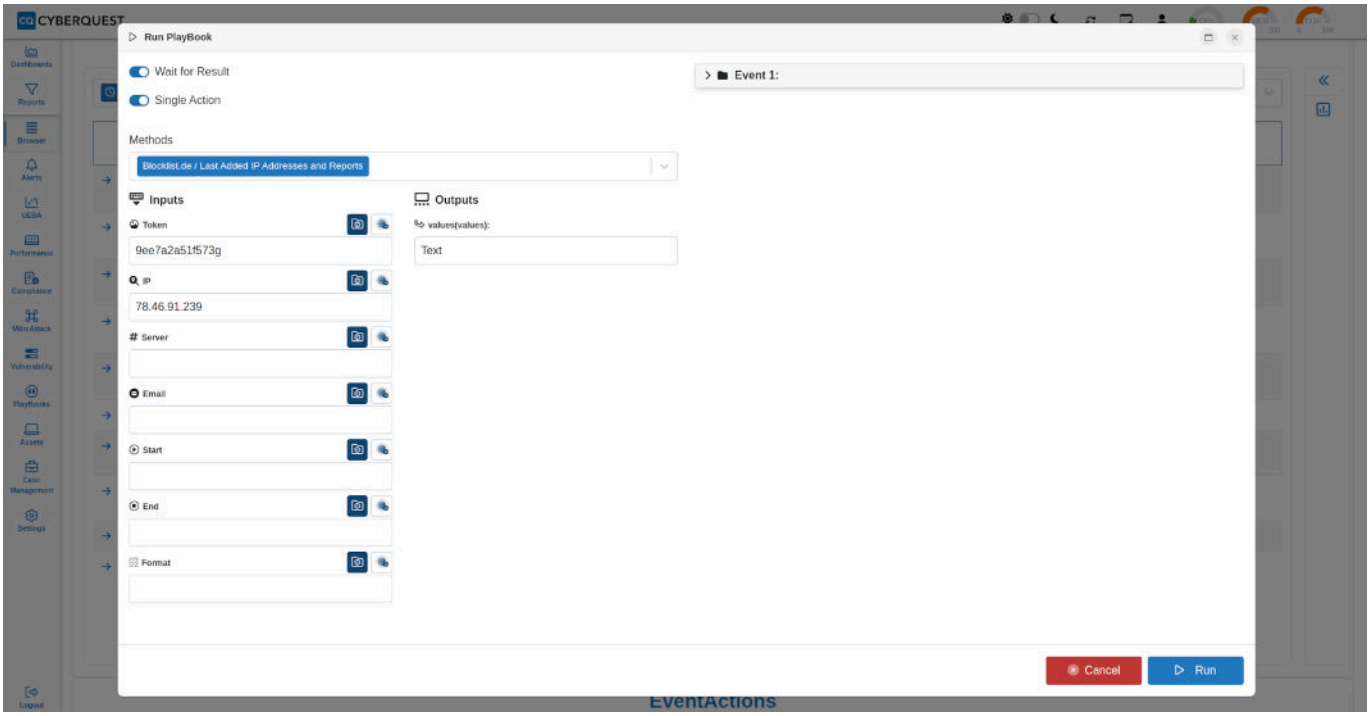


Inputs	Description
Token (is required)	To use the Blocklist.de API, you must have an API key
Time (is required)	The hour you want to see the last added IPs in the last 48 hours

Outputs	Description
values(values)	The results of the API call

Blocklist.de/Last Added IP Addresses and Reports method

The API can currently only issue attacks and reports per user, server or ip-address.



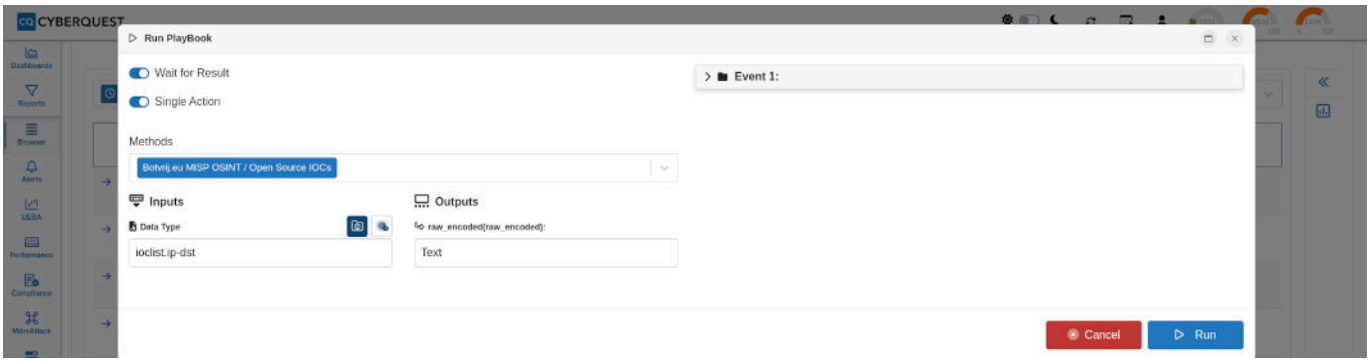
Inputs	Description
Token (is required)	To use the Blocklist.de API, you must have an API key
IP (is required)	IP-Address to check the Attacks
Server	ID of the server to query
Email	E-mail address of the user
Start	Start time as a Unix timestamp if the number is passed one is being sought for the first time
End	Should end as a Unix timestamp, to find where (End of Time-List)
Format	Output format: text (default, two rows), php (serialized), xml (xml file), json (json encoded)

Outputs	Description
values(values)	The results of the API call

BOTVRIJ.EU

Botvreij.eu MISP OSINT/Open Source IOCs method

Botvrij.eu provides different sets of open source IOCs that you can use in your security devices to detect possible malicious activity.



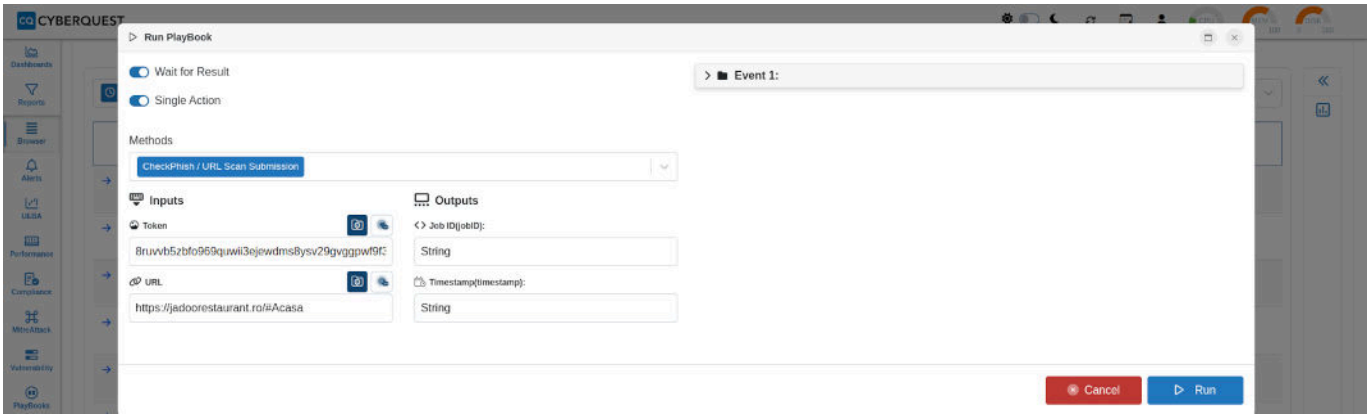
Inputs	Description
Data Type (is required)	The dataset you want to access

Outputs	Description
raw_encoded(raw_encoded)	The results of the API call

CheckPhish

CheckPhish/URL Scan Submission method

Submit URL for Scan.

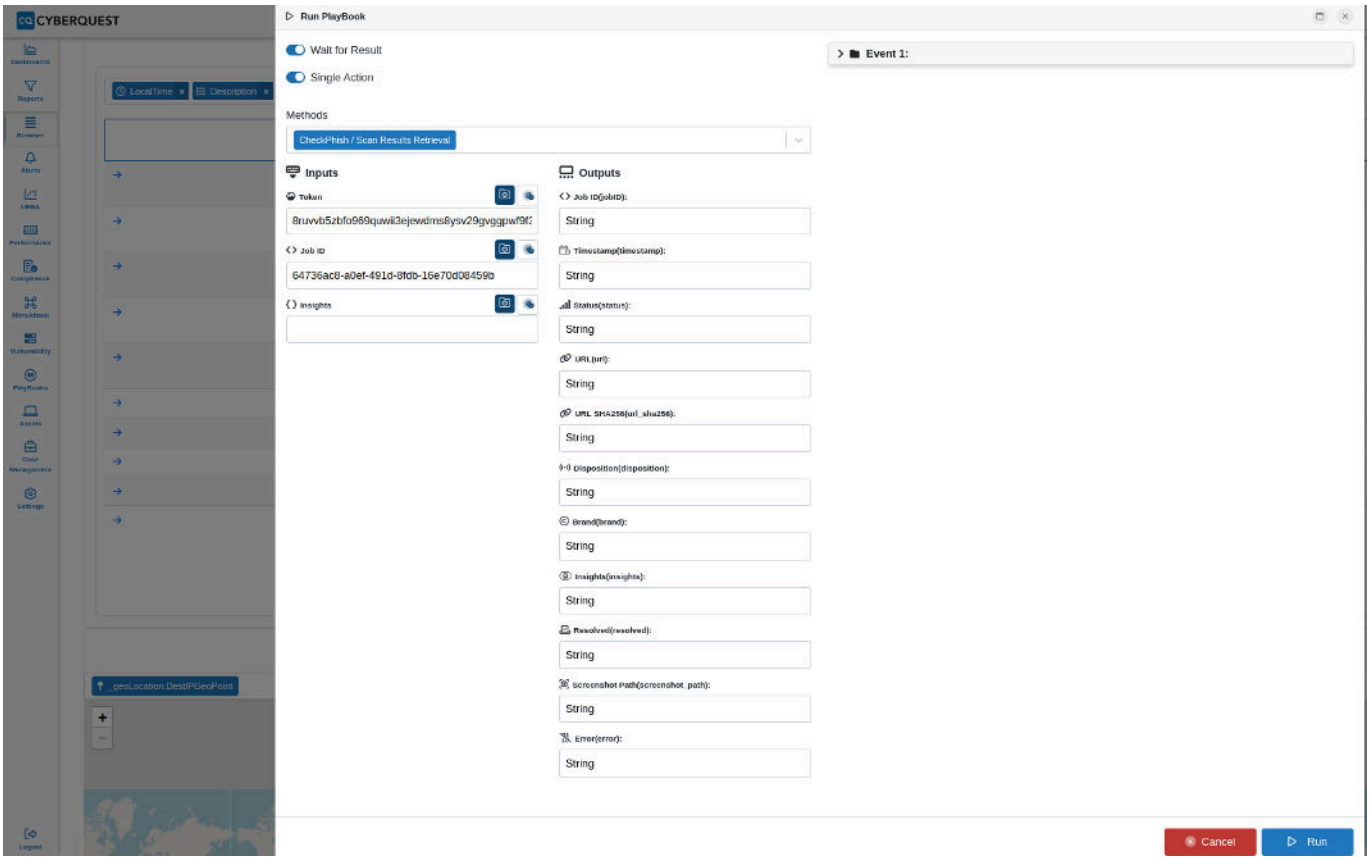


Inputs	Description
Token (is required)	To use the CheckPhish API, you must have an API key
URL (is required)	The URL which is submitted for analysis

Outputs	Description
Job ID(jobID)	jobID of the scan
Timestamp(timestamp)	Timestamp of when the scan the submission of report started

CheckPhish/Scan Results Retrieval method

Get API results from scan.



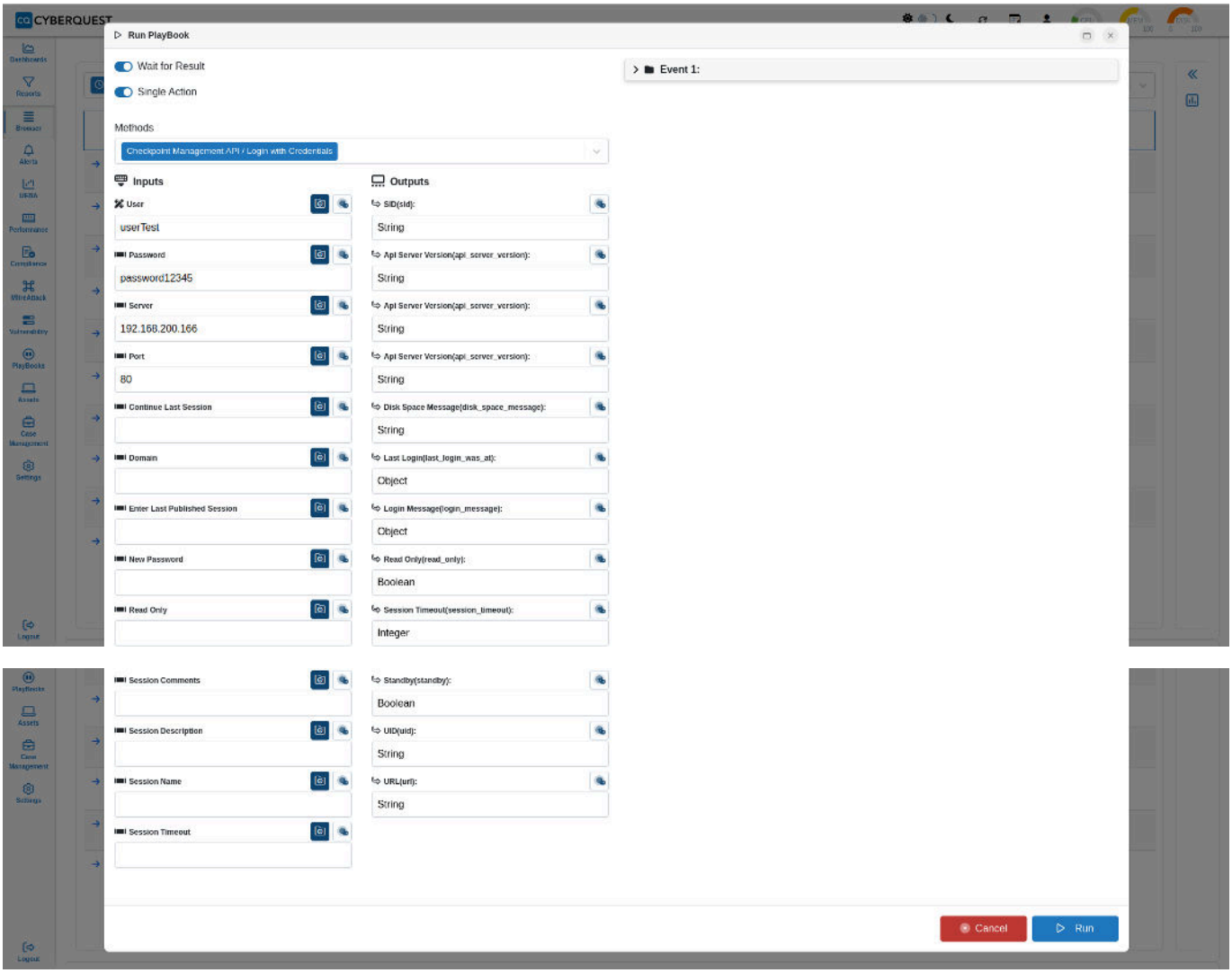
Inputs	Description
Token (is required)	To use the CheckPhish API, you must have an API key
Job ID (is required)	This parameter is used to identify the report of the URL submitted
Insights	Additional details for report

Outputs	Description
Job ID (jobID)	jobID of the scan
Timestamp (timestamp)	Timestamp of when the scan of report was finalised
Status (status)	Status of whether the job has completed. Returns DONE when completed
URL (url)	URL submitted for scanning
URL SHA256 (url_sha256)	SHA256 of the url submitted for scanning
Disposition (disposition)	The list of dispositions can be found below
Brand (brand)	Brand being targeted by the URL
Insights (insights)	insights link
Resolved (resolved)	True if the URL resolved. Else False
Screenshot Path (screenshot_path)	Storage location of the screenshot for the scan
Error (error)	False if the API call execution successfully, otherwise true

Checkpoint Management API

Checkpoint Management API/Login with Credentials method

Log in to the server with username and password. The server shows your session unique identifier. Enter this session unique identifier in the X-chkp-sid header of each request.

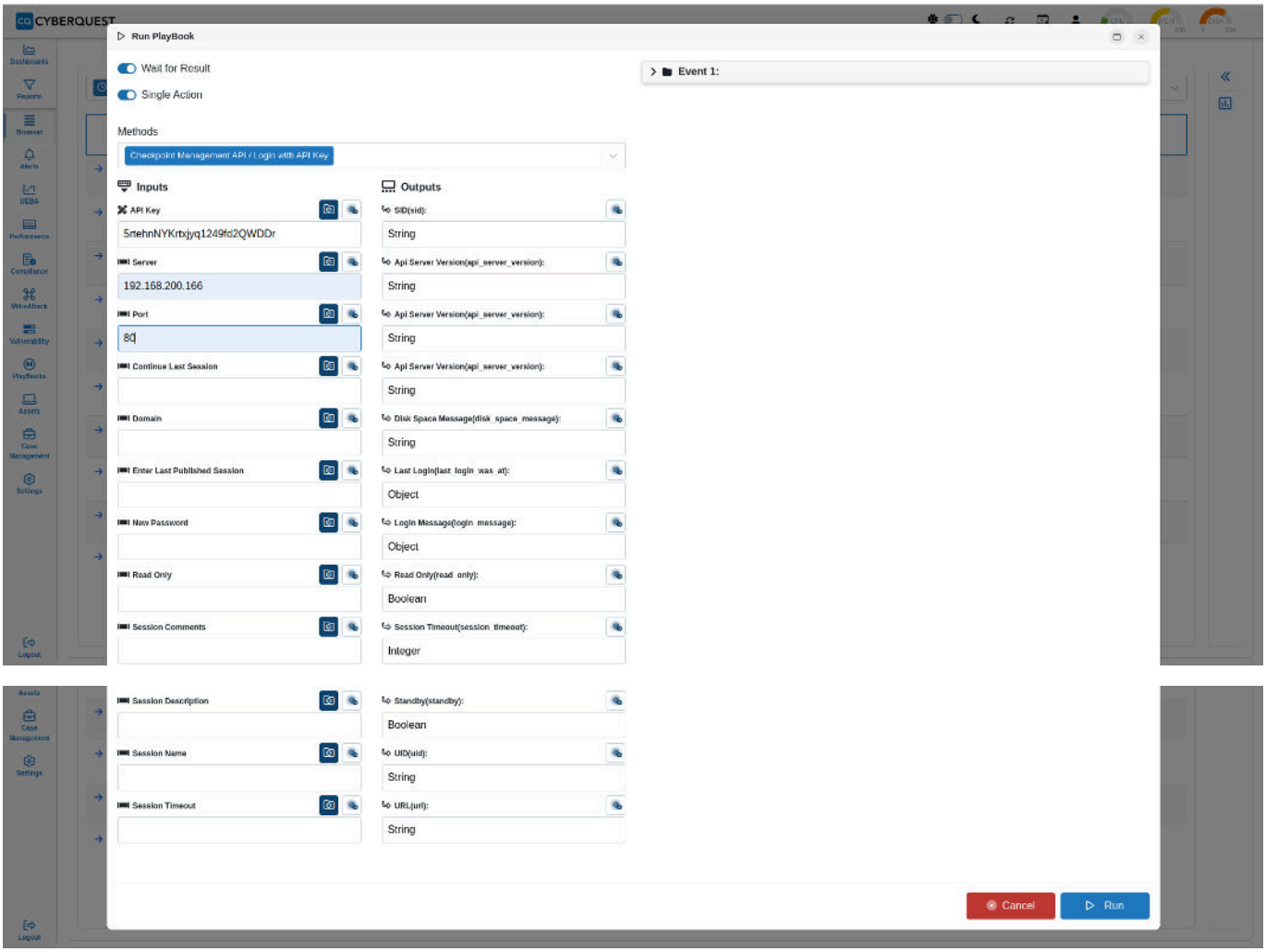

CYBERQUEST
Run PlayBook
Wait for Result
Single Action
Event 1:
Methods
Checkpoint Management API / Login with Credentials
Inputs
Outputs
User
userTest
Password
password12345
Server
192.168.200.166
Port
80
Continue Last Session
Domain
Enter Last Published Session
New Password
Read Only
Session Comments
Session Description
Session Name
Session Timeout
SID(sid):
String
Api Server Version(api_server_version):
String
Api Server Version(api_server_version):
String
Api Server Version(api_server_version):
String
Disk Space Message(disk_space_message):
String
Last Login(last_login_was_at):
Object
Login Message(login_message):
Object
Read Only(read_only):
Boolean
Session Timeout(session_timeout):
Integer
Standby(standby):
Boolean
UID(uid):
String
URL(url):
String
Cancel
Run

Inputs	Description
User (is required)	Administrator user name.
Password (is required)	Administrator password.
Server (is required)	Server Address
Port (is required)	Web Port
Continue Last Session	When continue-last-session is set to True, the new session would continue where the last session was stopped. This option is available when the administrator has only one session that can be continued. If there is more than one session, see switch-session API.
Domain	Use domain to login to specific domain. Domain can be identified by name or UID.
Enter Last Published Session	Login to the last published session. Such login is done with the Read Only permissions.
New Password	Administrator new password. Can only be used for first login, when the administrator password must be changed.
Read Only	Login with Read Only permissions. This parameter is not considered in case continue-last-session is true.
Session Comments	Session comments. Can be viewed only using the show-session API.
Session Description	A description of the sessions purpose.
Session Name	Session unique name.
Session Timeout	general: General metadata about the Correlation Rule

Outputs	Description
SID (sid)	Session unique identifier. Enter this session unique identifier in the X-chkp-sid header of each request
Api Server Version (api_server_version)	API Server version
Api Server Version (api_server_version)	API Server version
Api Server Version (api_server_version)	API Server version
Disk Space Message (disk_space_message)	Information about the available disk space on the management server
Last Login (last_login_was_at)	Timestamp when administrator last accessed the management server
Login Message (login_message)	Login message
Read Only (read_only)	True if this session is read only
Session Timeout (session_timeout)	Session expiration timeout in seconds
Standby (standby)	True if this management server is in the standby mode
UID (uid)	Session object unique identifier. This identifier may be used in the discard API to discard changes that were made in this session, when administrator is working from another session, or in the switch-session API
URL (url)	URL that was used to reach the API server

Checkpoint Management API/Login with API Key method

Log in to the server with username and password. The server shows your session unique identifier. Enter this session unique identifier in the X-chkp-sid header of each request.

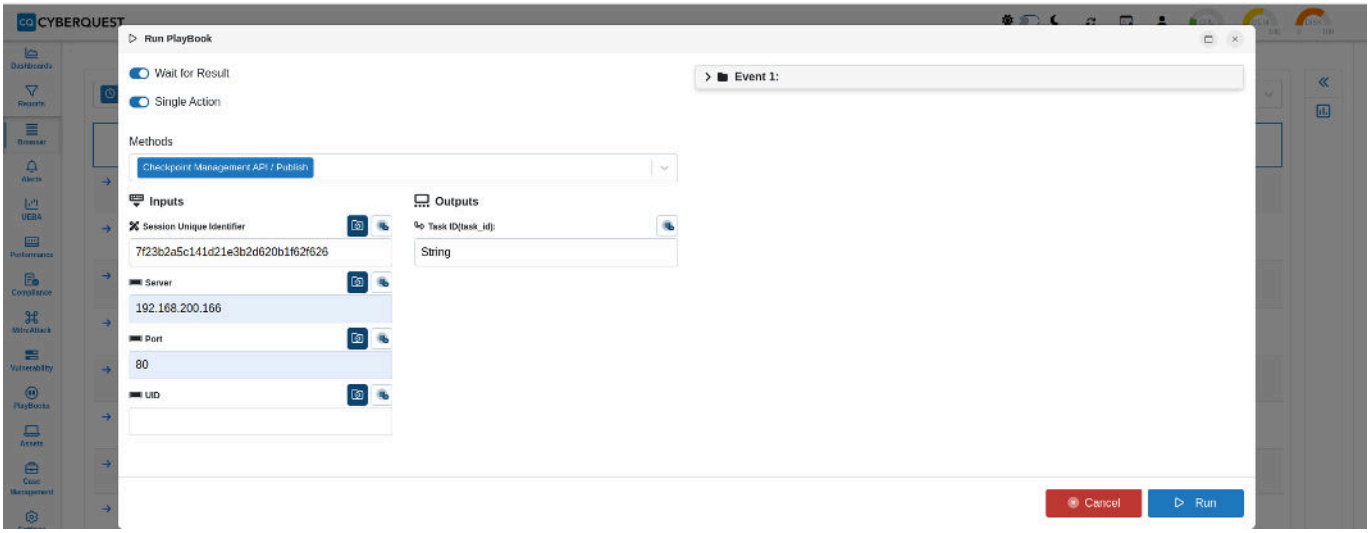


Inputs	Description
API Key (is required)	Administrator API key. When using api-key, there is no need to send user/password parameters.
Server (is required)	Server Address
Port (is required)	Web Port
Continue Last Session	When continue-last-session is set to True, the new session would continue where the last session was stopped. This option is available when the administrator has only one session that can be continued. If there is more than one session, see switch-session API.
Domain	Use domain to login to specific domain. Domain can be identified by name or UID.
Enter Last Published Session	Login to the last published session. Such login is done with the Read Only permissions.
New Password	Administrator new password. Can only be used for first login, when the administrator password must be changed.
Read Only	Login with Read Only permissions. This parameter is not considered in case continue-last-session is true.
Session Comments	Session comments. Can be viewed only using the show-session API.
Session Description	A description of the sessions purpose.
Session Name	Session unique name.
Session Timeout	general: General metadata about the Correlation Rule

Outputs	Description
SID (sid)	Session unique identifier. Enter this session unique identifier in the X-chkp-sid header of each request
Api Server Version (api_server_version)	API Server version
Api Server Version (api_server_version)	API Server version
Api Server Version (api_server_version)	API Server version
Disk Space Message (disk_space_message)	Information about the available disk space on the management server
Last Login (last_login_was_at)	Timestamp when administrator last accessed the management server
Login Message (login_message)	Login message
Read Only (read_only)	True if this session is read only
Session Timeout (session_timeout)	Session expiration timeout in seconds
Standby (standby)	True if this management server is in the standby mode
UID (uid)	Session object unique identifier. This identifier may be used in the discard API to discard changes that were made in this session, when administrator is working from another session, or in the switch-session API
URL (url)	URL that was used to reach the API server

Checkpoint Management API/Publish method

All the changes done by this user will be seen by all users only after publish is called.

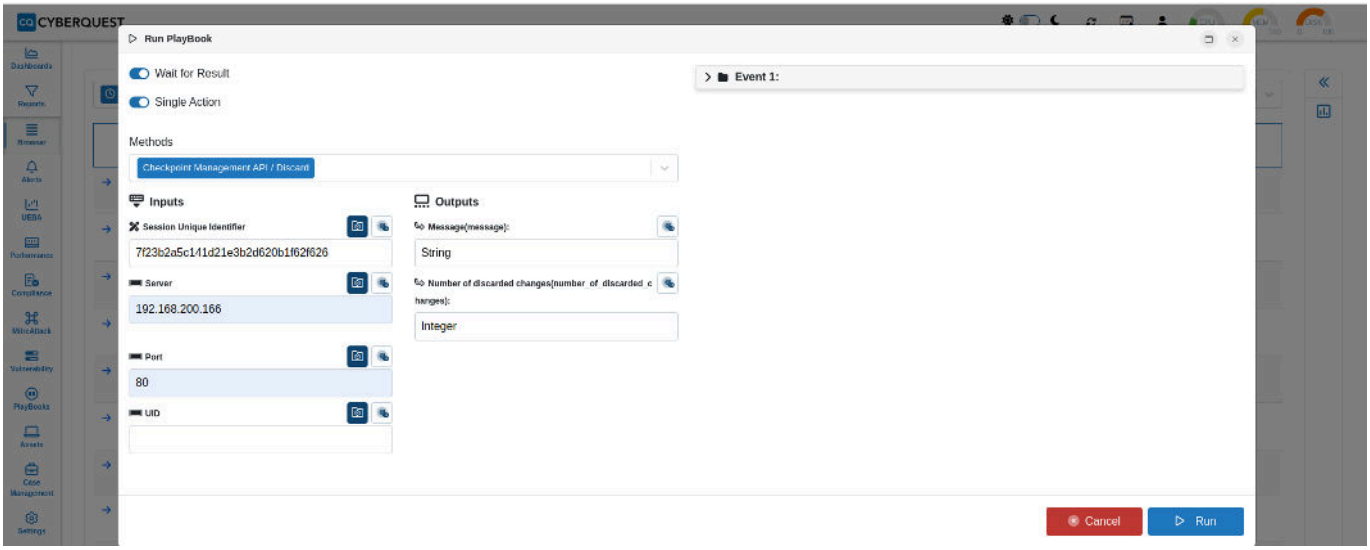


Inputs	Description
Session Unique Identifier (is required)	Session unique identifier as it returned by the login request
Server (is required)	Server Address
Port (is required)	Web Port
UID	Session unique identifier. Specify it to publish a different session than the one you currently use

Outputs	Description
Task ID (task_id)	Publish task UID. Use show-task command to check the progress of the task

Checkpoint Management API/Discard method

All changes done by user are discarded and removed from database.

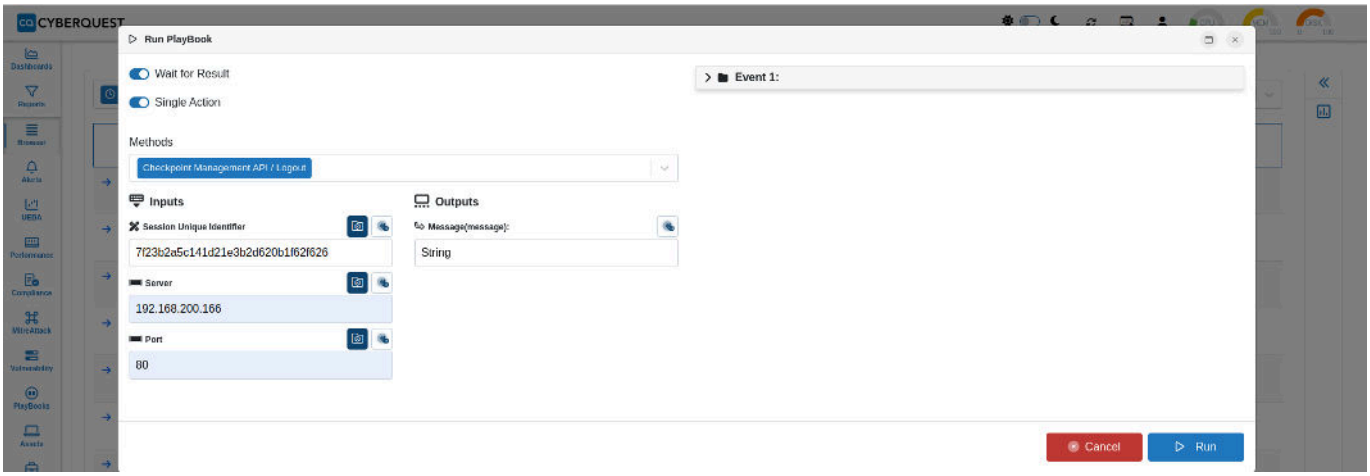


Inputs	Description
Session Unique Identifier (is required)	Session unique identifier as it returned by the login request
Server (is required)	Server Address
Port (is required)	Web Port
UID	Session unique identifier. Specify it to discard a different session than the one you currently use

Outputs	Description
Message (message)	Publish task UID. Use show-task command to check the progress of the task
Number of discarded changes (number_of_discarded_changes)	Publish task UID. Use show-task command to check the progress of the task

Checkpoint Management API/Logout method

Log out from the current session. After logging out the session id is not valid any more.

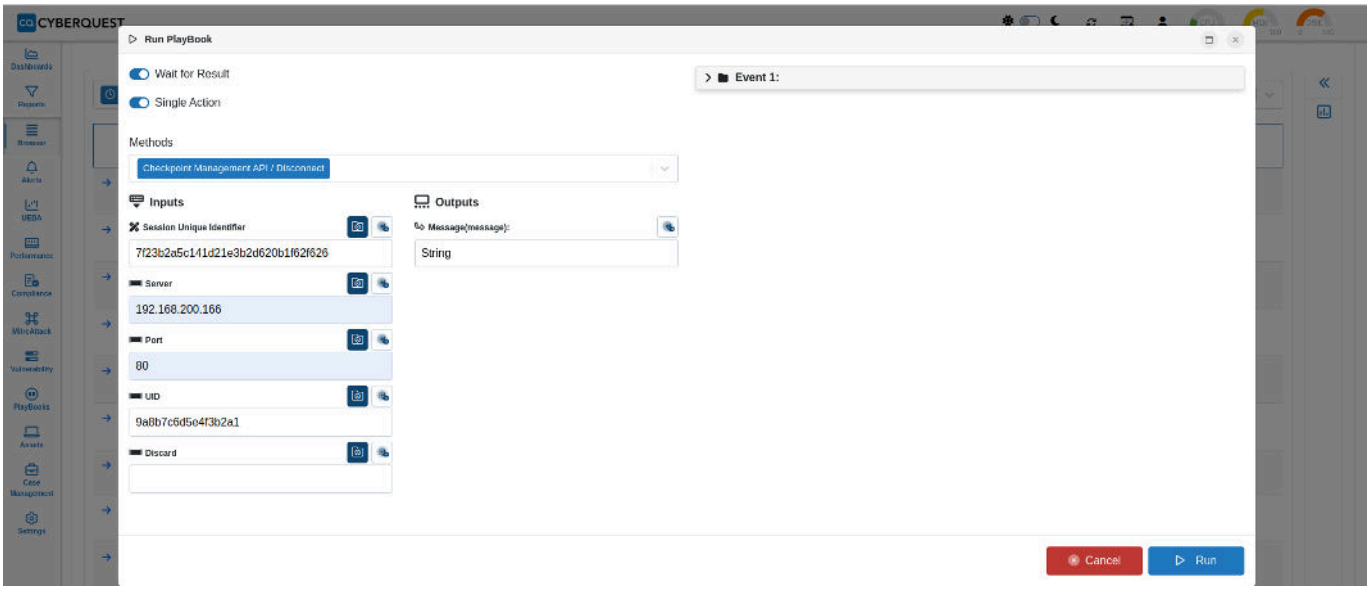


Inputs	Description
Session Unique Identifier (is required)	Session unique identifier as it returned by the login request
Server (is required)	Server Address
Port (is required)	Web Port

Outputs	Description
Message (message)	Operation status

Checkpoint Management API/Disconnect method

Disconnect a private session.

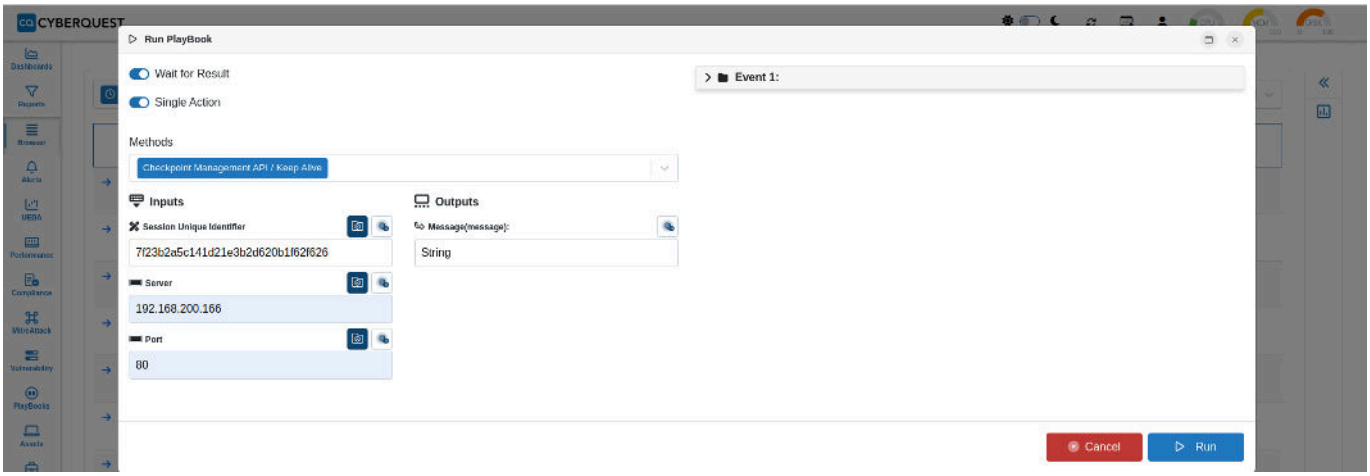


Inputs	Description
Session Unique Identifier (is required)	Session unique identifier as it returned by the login request
Server (is required)	Server Address
Port (is required)	Web Port
UID (is required)	Session unique identifier
Discard	Discard all changes committed during the session

Outputs	Description
Message (message)	Operation status

Checkpoint Management API/Keep Alive method

Keep the session valid/alive.

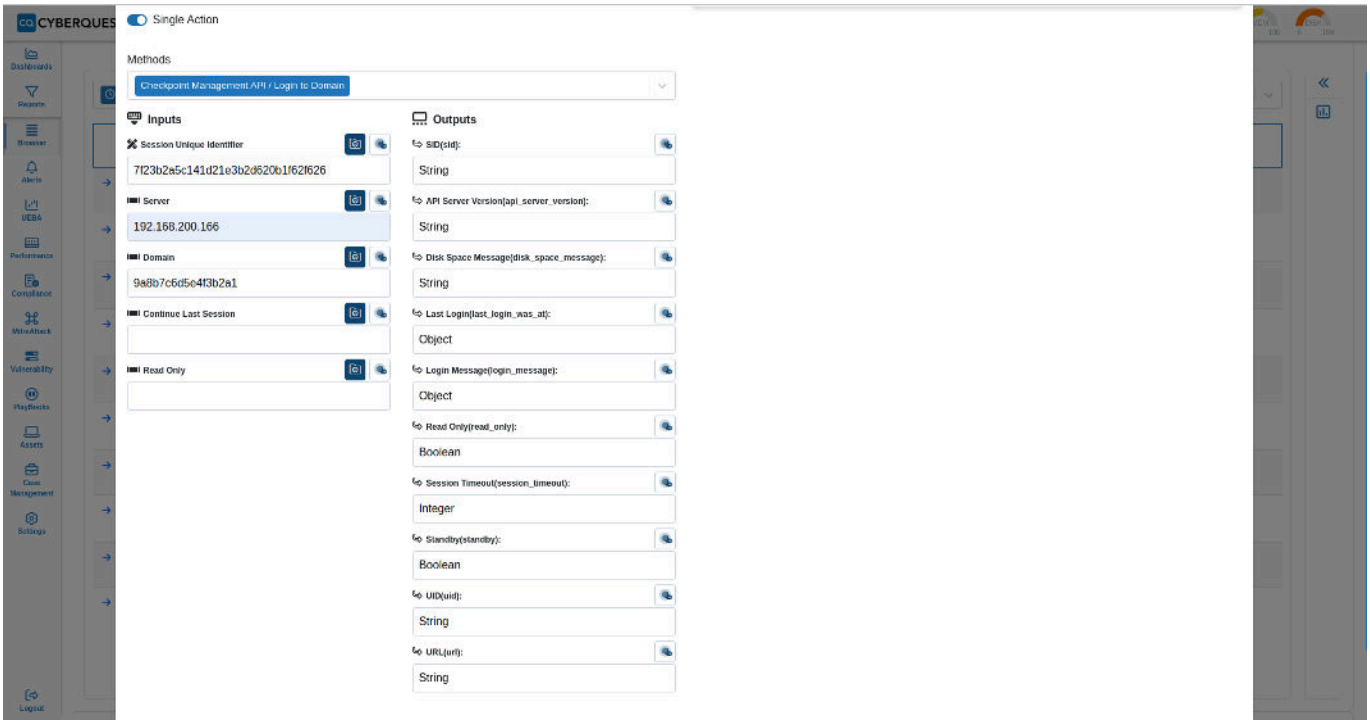


Inputs	Description
Session Unique Identifier (is required)	Session unique identifier as it returned by the login request
Server (is required)	Server Address
Port (is required)	Web Port

Outputs	Description
Message (message)	Operation status

Checkpoint Management API/Login to Domain method

Login from MDS to other domain.This command is available only after logging in to the System Data domain.

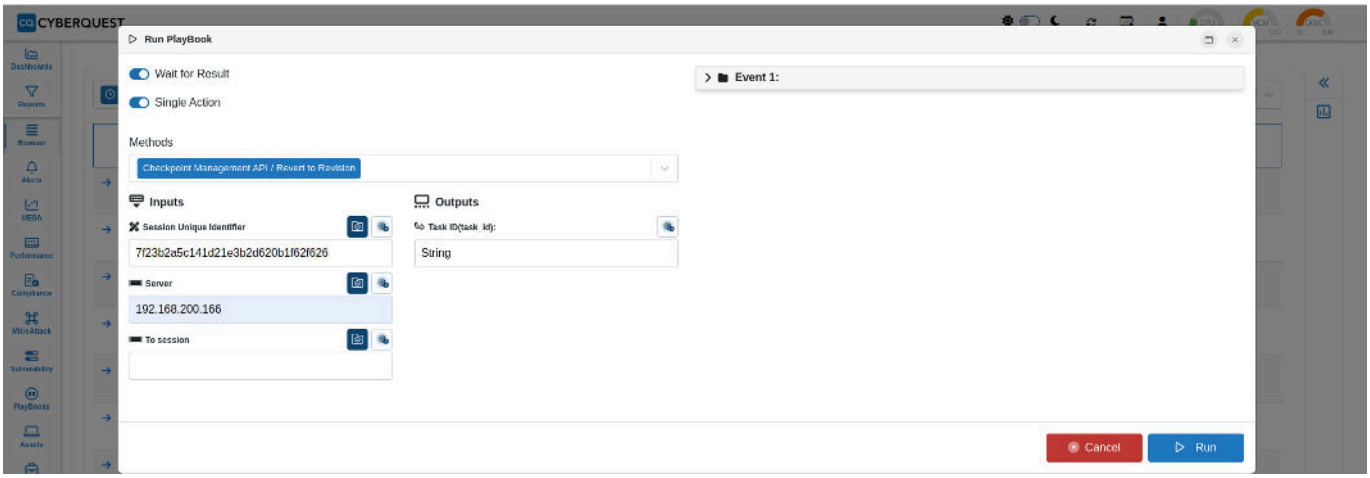


Inputs	Description
Session Unique Identifier (is required)	Session unique identifier as it returned by the login request
Server (is required)	Server Address
Domain (is required)	Domain identified by the name or UID
Continue Last Session	When continue-last-session is set to True, the new session would continue where the last session was stopped. This option is available when the administrator has only one session that can be continued. If there is more than one session, see switch-session API
Read Only	Login with Read Only permissions. This parameter is not considered in case continue-last-session is true

Outputs	Description
SID (sid)	Session unique identifier. Enter this session unique identifier in the X-chkp-sid header of each request
API Server Version (api_server_version)	API Server version
Disk Space Message (disk_space_message)	Information about the available disk space on the management server
Last Login (last_login_was_at)	Timestamp when administrator last accessed the management server
Login Message (login_message)	Login message
Read Only (read_only)	True if this session is read only.
Session Timeout (session_timeout)	Session expiration timeout in seconds
Standby (standby)	True if this management server is in the standby mode
UID (uid)	Session object unique identifier. This identifier may be used in the discard API to discard changes that were made in this session, when administrator is working from another session, or in the switch-session API
URL (url)	URL that was used to reach the API server

Checkpoint Management API/Revert to Revision method

Revert the Management Database to the selected revision.

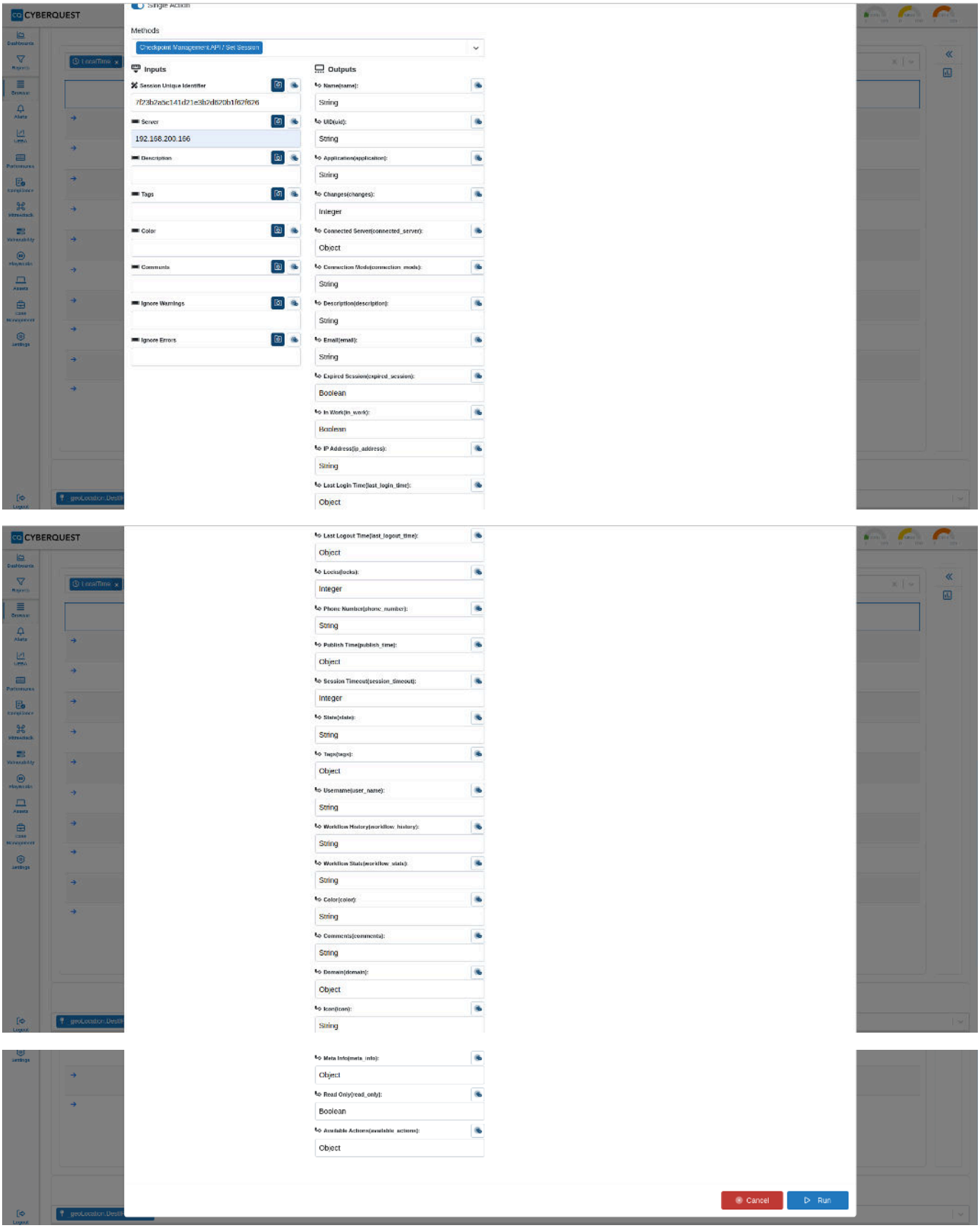


Inputs	Description
Session Unique Identifier (is required)	Session unique identifier as it returned by the login request
Server (is required)	Server Address
To session	Session unique identifier. Specify the session id you would like to revert your database to

Outputs	Description
Task ID (task_id)	Asynchronous task unique identifier. Use show-task command to check the progress of the task

Checkpoint Management API/Set Session method

Edit users current session.

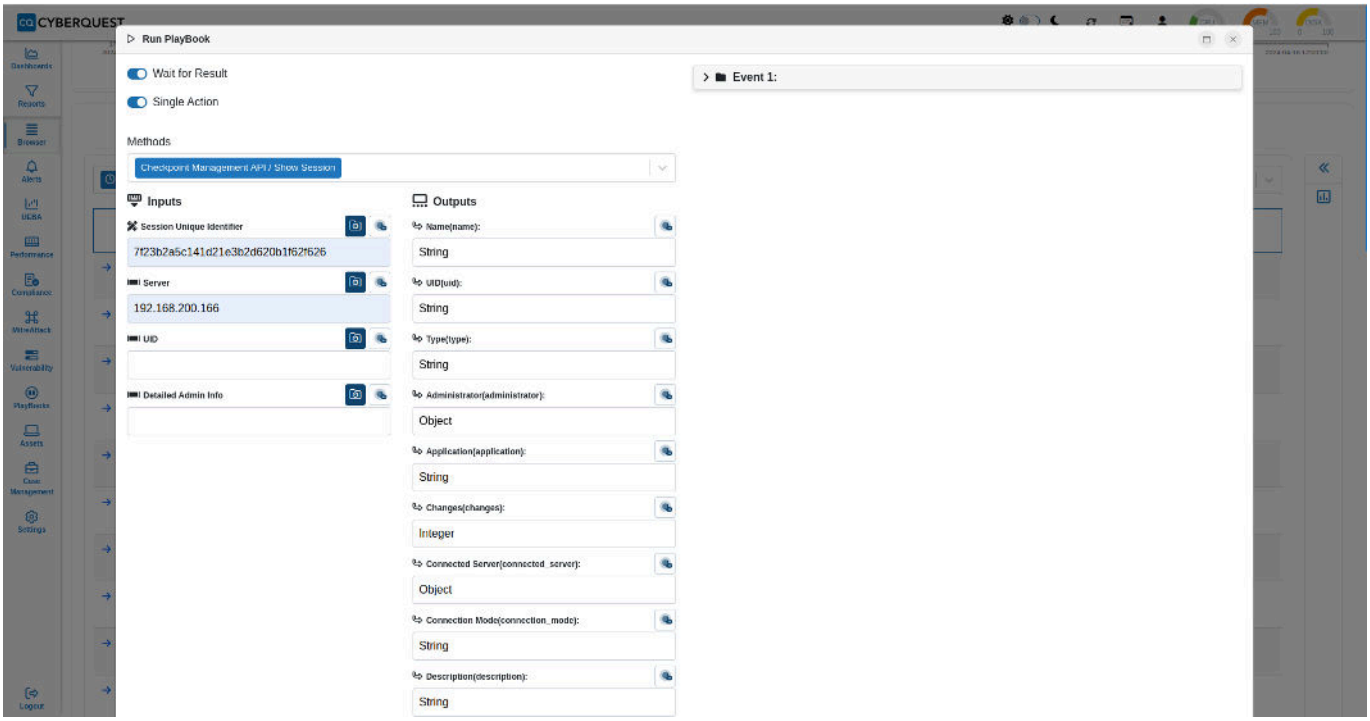

CYBERQUEST
Single Action
Methods
Checkpoint Management API / Set Session
Inputs
Session Unique Identifier
7f23b2a5c141d21e3b2d820b1f62f626
Server
192.168.200.166
Description
Tags
Color
Comments
Ignore Warnings
Ignore Errors
Outputs
Name(name):
String
UID(uid):
String
Application(application):
String
Changes(changes):
Integer
Connected Server(connected_server):
Object
Connection Mode(connection_mode):
String
Description(description):
String
Email(email):
String
Expired Session(expired_session):
Boolean
In Work(in_work):
Boolean
IP Address(ip_address):
String
Last Login Time(last_login_time):
Object
Last Logout Time(last_logout_time):
Object
Locks(locks):
Integer
Phone Number(phone_number):
String
Publish Time(publish_time):
Object
Session Timeout(session_timeout):
Integer
State(state):
String
Tags(tags):
Object
Username(user_name):
String
Workflow History(workflow_history):
String
Workflow State(workflow_state):
String
Color(color):
String
Comments(comments):
String
Domain(domain):
Object
Icon(icon):
String
Meta Info(meta_info):
Object
Read Only(read_only):
Boolean
Available Actions(available_actions):
Object
Cancel
Run

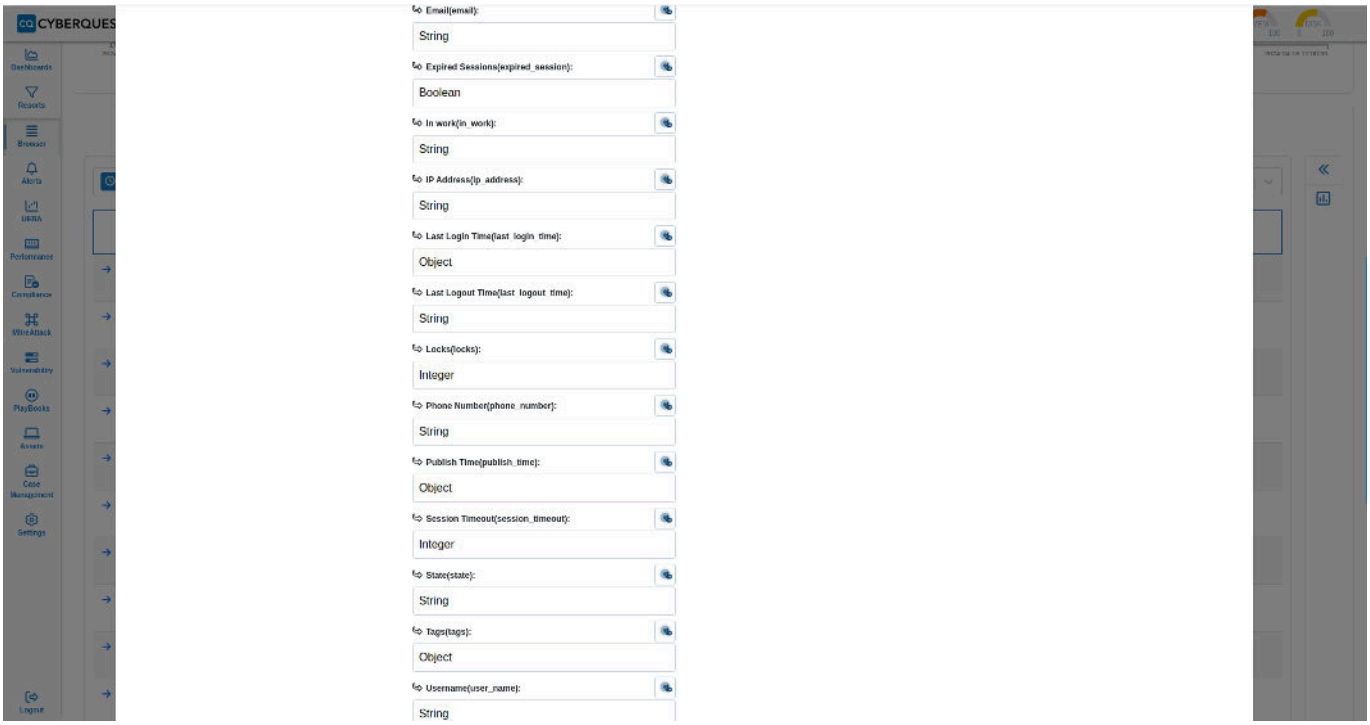
Inputs	Description
Session Unique Identifier (is required)	Session unique identifier as it returned by the login request
Server (is required)	Server Address
Description	Session description
Tags	Collection of tag identifiers
Color	Color of the object. Should be one of existing colors
Comments	Comments string
Ignore Warnings	Apply changes ignoring warnings
Ignore Errors	Apply changes ignoring errors. You wont be able to publish such a changes. If ignore-warnings flag was omitted - warnings will also be ignored

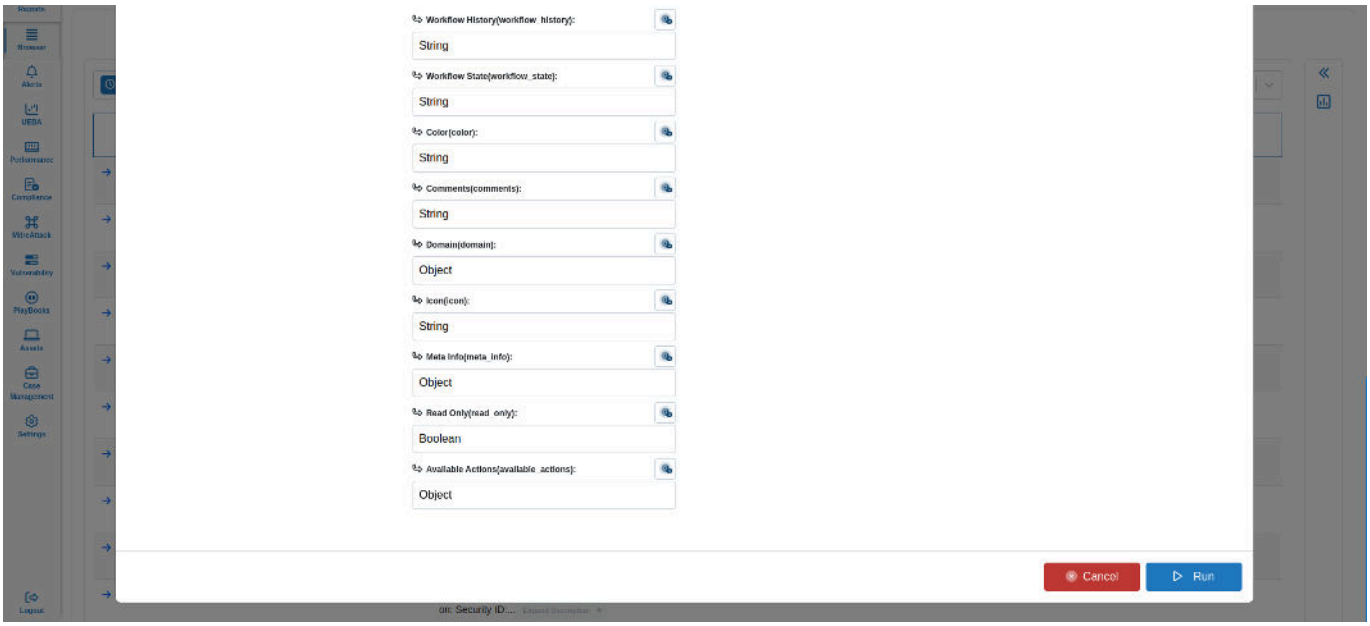
Outputs	Description
Name (name)	Object name. Must be unique in the domain
UID (uid)	Object unique identifier
Application (application)	The name of the application serving the Management API requests.
Changes (changes)	Asynchronous task unique identifier. Use show-task command to check the progress of the task.
Connected Server (connected_server)	The server which the user is currently connected to.
Connection Mode (connection_mode)	Session connection mode.
Description (description)	Session description.
Email (email)	Administrator email.
Expired Session (expired_session)	True if the session is expired.
In Work (in_work)	True if the session is in work state.
IP Address (ip_address)	IP address from which the session was initiated.
Last Login Time (last_login_time)	Session description
Last Logout Time (last_logout_time)	Timestamp when user last accessed the management server.
Locks (locks)	Number of locked objects.
Phone Number (phone_number)	Administrator phone number.
Publish Time (publish_time)	Timestamp when user published changes on the management server.
Session Timeout (session_timeout)	Session expiration timeout in seconds.
State (state)	Session state.
Tags (tags)	Collection of tag objects identified by the name or UID. Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.
Username (user_name)	The name of the logged in user.
Workflow History (workflow_history)	Show details per each workflow action.
Workflow State (workflow_state)	Workflow session state.
Color (color)	Color of the object. Should be one of existing colors.
Comments (comments)	Comments string.
Domain (domain)	Asynchronous task unique identifier. Use show-task command to check the progress of the task.
Icon (icon)	Object icon.
Meta Info (meta_info)	Object metadata.
Read Only (read_only)	Asynchronous task unique identifier. Use show-task command to check the progress of the task.
Available Actions (available_actions)	Actions that are available on the object.

Checkpoint Management API/Show Session method

Show session.


CYBERQUEST
Run PlayBook
Wait for Result
Single Action
Methods
Checkpoint Management API / Show Session
Inputs
Session Unique Identifier
7f23b2a5c141d21e3b2d620b1f62f626
Server
192.168.200.166
UID
Detailed Admin Info
Outputs
Name(name):
String
UID(uid):
String
Type(type):
String
Administrator(administrator):
Object
Application(application):
String
Changes(changes):
Integer
Connected Server(connected_server):
Object
Connection Mode(connection_mode):
String
Description(description):
String
Event 1:


Email(email):
String
Expired Sessions(expired_session):
Boolean
In work(in_work):
String
IP Address(ip_address):
String
Last Login Time(last_login_time):
Object
Last Logout Time(last_logout_time):
String
Locks(locks):
Integer
Phone Number(phone_number):
String
Publish Time(publish_time):
Object
Session Timeout(session_timeout):
Integer
State(state):
String
Tags(tags):
Object
Username(user_name):
String

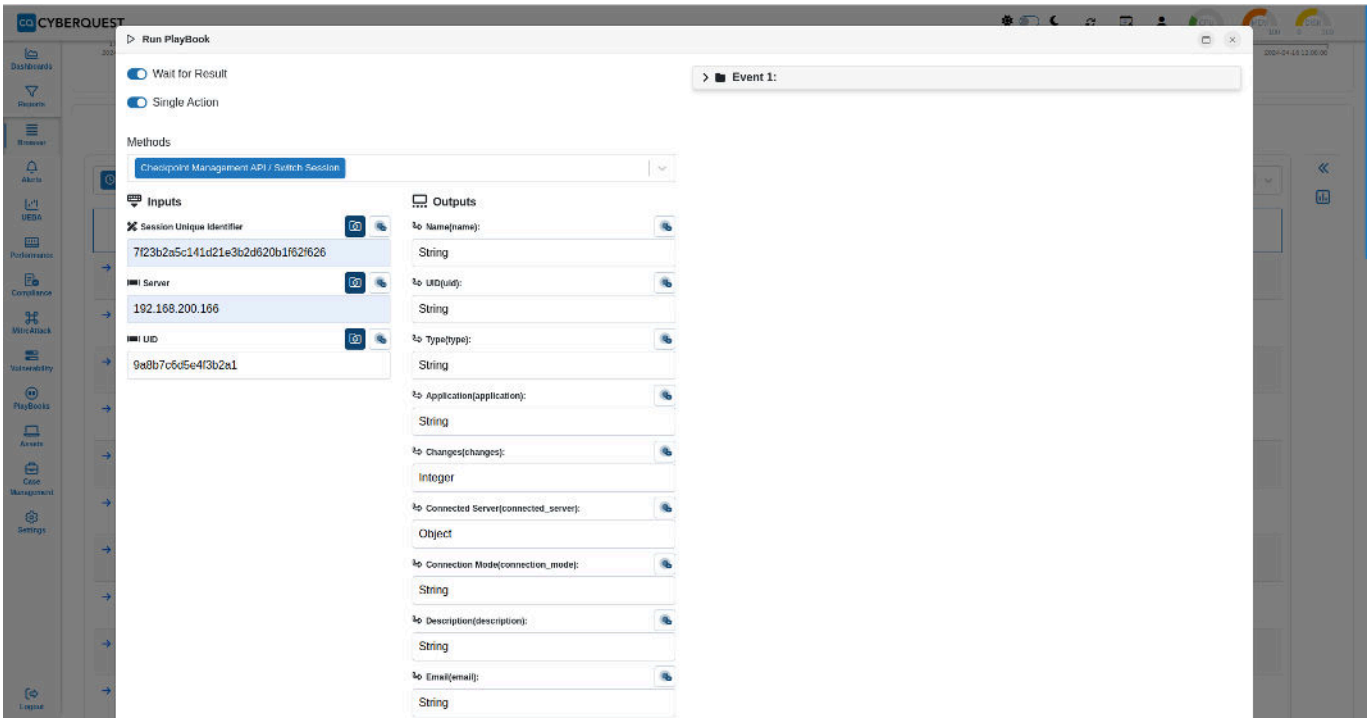


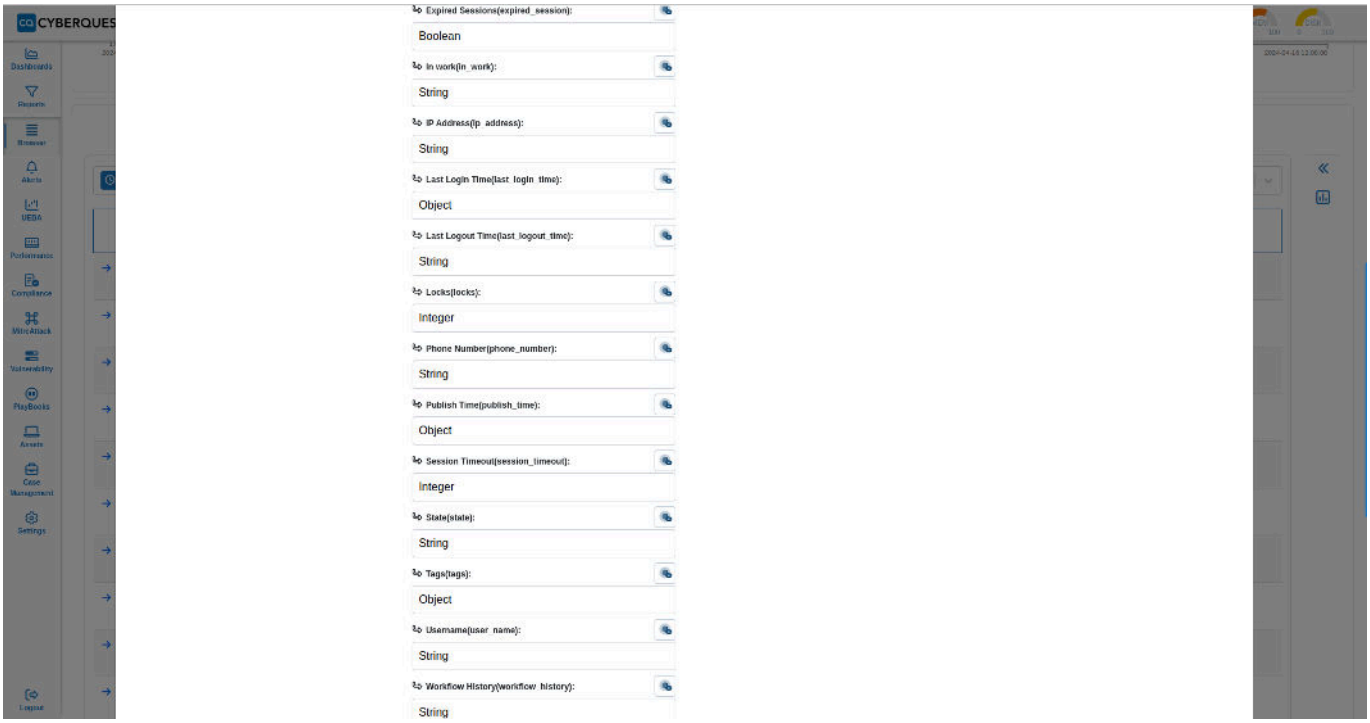
Inputs	Description
Session Unique Identifier (is required)	Session unique identifier as it returned by the login request
Server (is required)	Server Address
UID	Session unique identifier
Detailed Admin Info	Session unique identifier. Specify the session id you would like to revert your database to

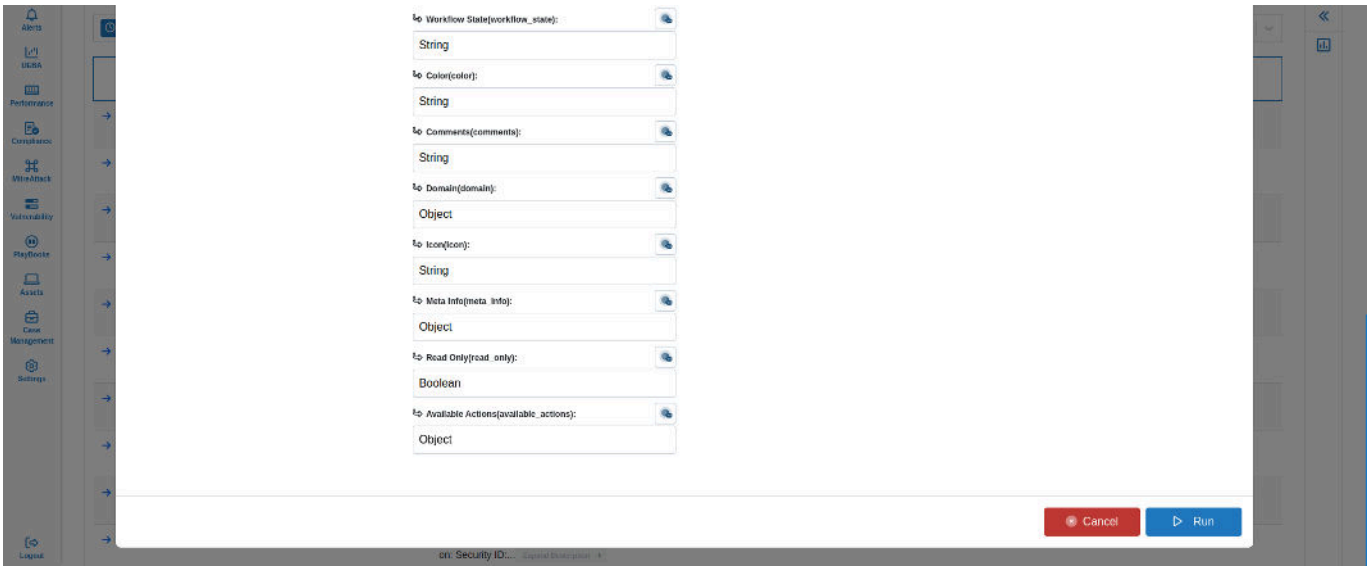
Outputs	Description
Name (name)	Object name. Must be unique in the domain.
UID (uid)	Object unique identifier
Type (type)	Object type
Administrator (administrator)	Asynchronous task unique identifier. Use show-task command to check the progress of the task
Application (application)	The name of the application serving the Management API requests
Changes (changes)	Asynchronous task unique identifier. Use show-task command to check the progress of the task.
Connected Server (connected_server)	The server which the user is currently connected to
Connection Mode (connection_mode)	Session connection mode
Description (description)	Session description
Email (email)	Administrator email
Expired Sessions (expired_session)	True if the session is expired
In work (in_work)	True if the session is in work state
IP Address (ip_address)	IP address from which the session was initiated
Last Login Time (last_login_time)	Session description
Last Logout Time (last_logout_time)	Timestamp when user last accessed the management server
Locks (locks)	Number of locked objects
Phone Number (phone_number)	Administrator phone number
Publish Time (publish_time)	Timestamp when user published changes on the management server
Session Timeout (session_timeout)	Session expiration timeout in seconds
State (state)	Session state
Tags (tags)	Asynchronous task unique identifier. Use show-task command to check the progress of the task
Username (user_name)	The name of the logged in user
Workflow History (workflow_history)	Show details per each workflow action
Workflow State (workflow_state)	Workflow session state
Color (color)	Color of the object. Should be one of existing colors
Comments (comments)	Comments string
Domain (domain)	Asynchronous task unique identifier. Use show-task command to check the progress of the task
Icon (icon)	Object icon
Meta Info (meta_info)	Object metadata
Read Only (read_only)	Asynchronous task unique identifier. Use show-task command to check the progress of the task
Available Actions (available_actions)	Actions that are available on the object

Checkpoint Management API/Switch Session method

Switch to a disconnected Management API session of the same administrator. To switch to an open session or to a session of a different administrator use the take-over session API.


CYBERQUEST
Run PlayBook
Wait for Result
Single Action
Methods
Checkpoint Management API / Switch Session
Inputs
Session Unique Identifier
7f23b2a5c141d21e3b2d620b1f62f626
Server
192.168.200.166
UID
9a8b7c6d5e4f3b2a1
Outputs
Event 1:
Name(name):
String
UID(uid):
String
Type(type):
String
Application(application):
String
Changes(changes):
Integer
Connected Server(connected_server):
Object
Connection Mode(connection_mode):
String
Description(description):
String
Email(email):
String


Expired Sessions(expired_session):
Boolean
In work(in_work):
String
IP Address(ip_address):
String
Last Login Time(last_login_time):
Object
Last Logout Time(last_logout_time):
String
Locks(locks):
Integer
Phone Number(phone_number):
String
Publish Time(publish_time):
Object
Session Timeout(session_timeout):
Integer
State(state):
String
Tags(tags):
Object
Username(user_name):
String
Workflow History(workflow_history):
String

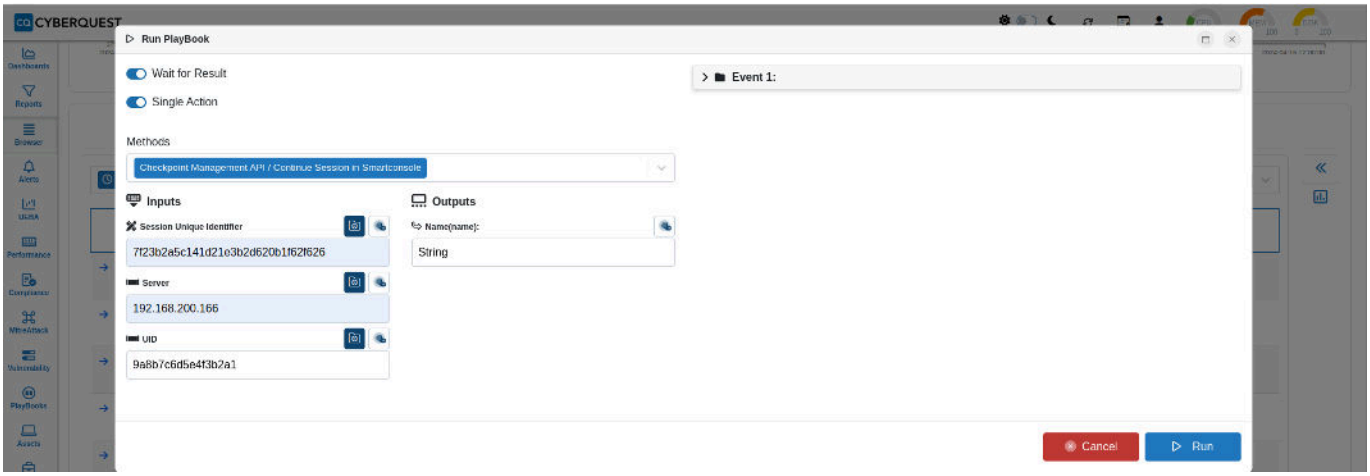


Inputs	Description
Session Unique Identifier (is required)	Session unique identifier as it returned by the login request
Server (is required)	Server Address
UID (is required)	Session unique identifier.

Outputs	Description
Name (name)	Object name. Must be unique in the domain.
UID (uid)	Object unique identifier
Type (type)	Object type.
Application (application)	The name of the application serving the Management API requests
Changes (changes)	Asynchronous task unique identifier. Use show-task command to check the progress of the task.
Connected Server (connected_server)	The server which the user is currently connected to
Connection Mode (connection_mode)	Session connection mode.
Description (description)	Session description.
Email (email)	Administrator email.
Expired Sessions (expired_session)	True if the session is expired.
In work (in_work)	True if the session is in work state.
IP Address (ip_address)	IP address from which the session was initiated.
Last Login Time (last_login_time)	Session description
Last Logout Time (last_logout_time)	Timestamp when user last accessed the management server.
Locks (locks)	Number of locked objects.
Phone Number (phone_number)	Administrator phone number.
Publish Time (publish_time)	Timestamp when user published changes on the management server.
Session Timeout (session_timeout)	Session expiration timeout in seconds.
State (state)	Session state.
Tags (tags)	Asynchronous task unique identifier. Use show-task command to check the progress of the task.
Username (user_name)	The name of the logged in user.
Workflow History (workflow_history)	Show details per each workflow action.
Workflow State (workflow_state)	Workflow session state.
Color (color)	Color of the object. Should be one of existing colors.
Comments (comments)	Comments string.
Domain (domain)	Asynchronous task unique identifier. Use show-task command to check the progress of the task.
Icon (icon)	Object icon.
Meta Info (meta_info)	Object metadata.
Read Only (read_only)	Asynchronous task unique identifier. Use show-task command to check the progress of the task.
Available Actions (available_actions)	Actions that are available on the object.

Checkpoint Management API/Continue Session in Smartconsole method

Logout from existing session. The session will be continued next time your open SmartConsole. In case uid is not provided, use current session. In order for the session to pass successfully to SmartConsole, make sure you dont have any other active GUI sessions.



Inputs	Description
Session Unique Identifier (is required)	Session unique identifier as it returned by the login request
Server (is required)	Server Address
UID	Session unique identifier.

Outputs	Description
Name (name)	Object name. Must be unique in the domain.

Checkpoint Management API/Show Sessions method

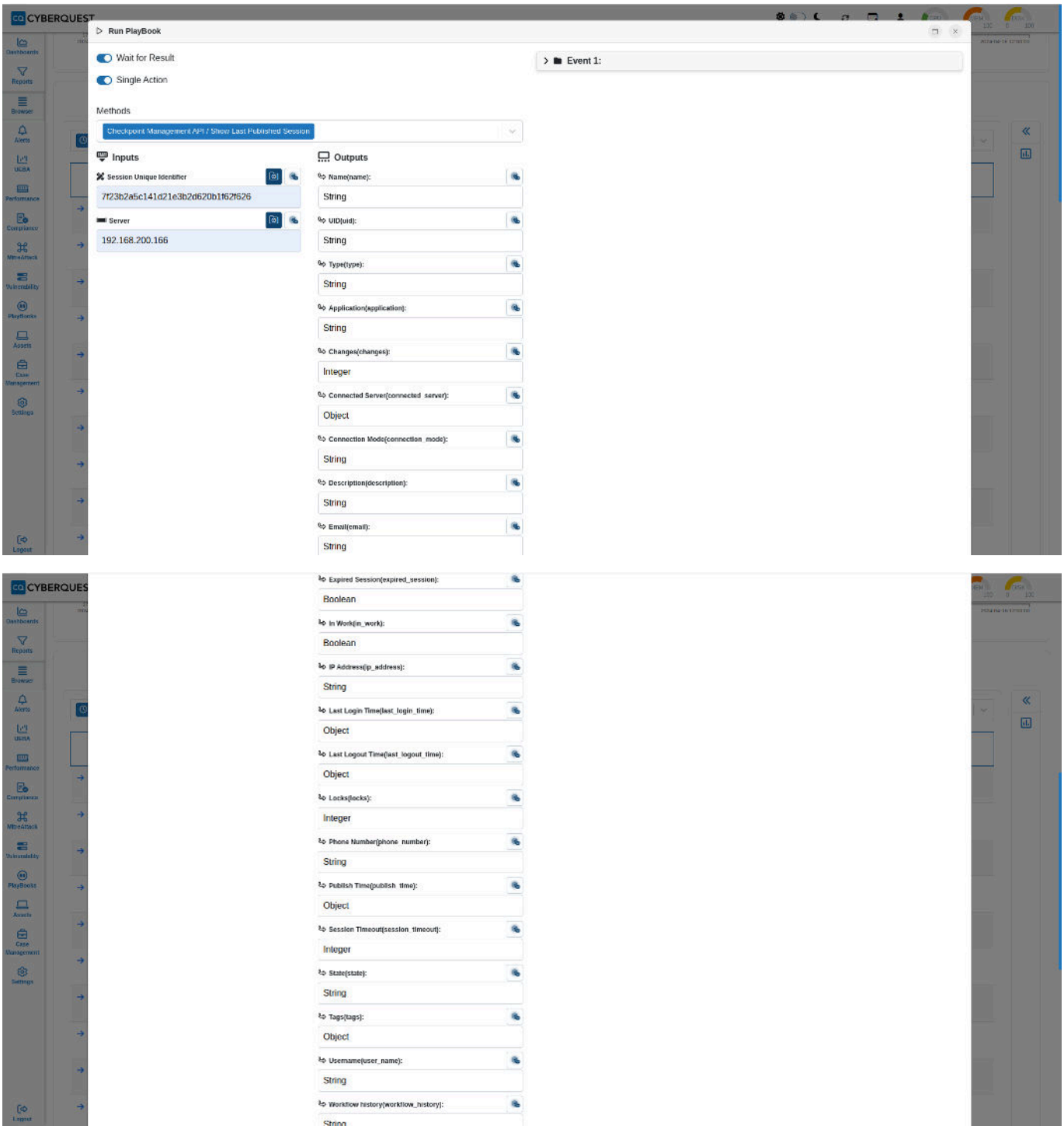
Retrieve all objects.

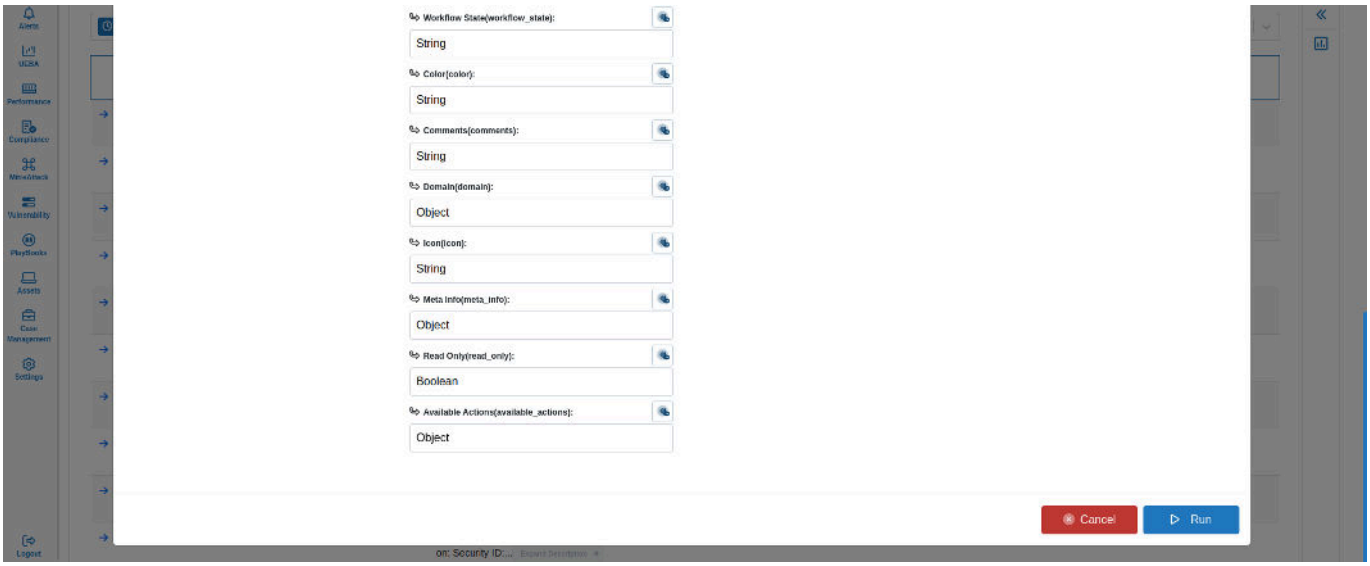
Inputs	Description
Session Unique Identifier (is required)	Session unique identifier as it returned by the login request
Server (is required)	Server Address
Filter	Search expression to filter objects by. The provided text should be exactly the same as it would be given in SmartConsole Object Explorer. The logical operators in the expression (AND, OR) should be provided in capital letters. The search involves both a IP search and a textual search in name, comment, tags etc.
Limit	The maximal number of returned results.
Offset	Number of the results to initially skip.
Order	Sorts results by the given field. By default the results are sorted in the descending order by the session publish time.
View Published Sessions	Show a list of published sessions.
Details Level	he level of detail for some of the fields in the response can vary from showing only the UID value of the object to a fully detailed representation of the object.

Outputs	Description
From (from)	From which element number the query was done.
Objects (objects)	Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.
To (to)	To which element number the query was done.
Total (total)	Total number of elements returned by the query.

Checkpoint Management API/Show Last Published Session method

Shows the last published session.



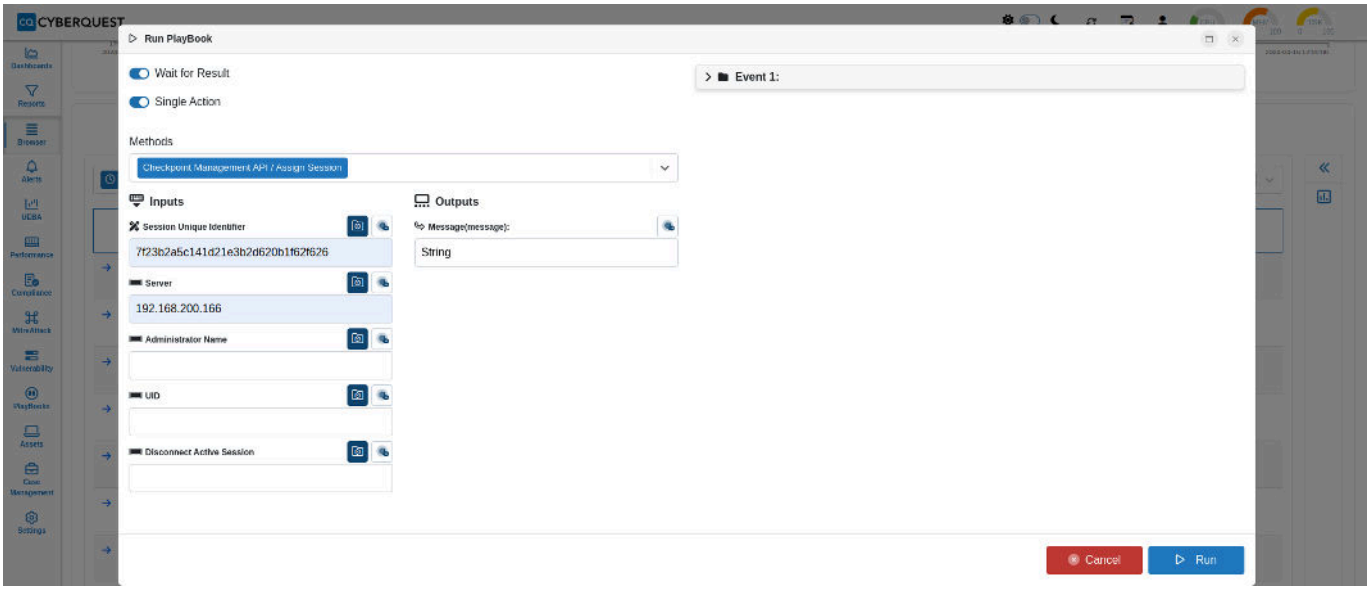


Inputs	Description
Session Unique Identifier (is required)	Session unique identifier as it returned by the login request
Server (is required)	Server Address

Outputs	Description
Name (name)	Object name. Must be unique in the domain.
UID (uid)	Object unique identifier.
Type (type)	Object type.
Application (application)	The name of the application serving the Management API requests.
Changes (changes)	Number of pending changes.
Connected Server (connected_server)	The server which the user is currently connected to.
Connection Mode (connection_mode)	Session connection mode.
Description (description)	Session description.
Email (email)	Administrator email.
Expired Session (expired_session)	True if the session is expired.
In Work (in_work)	True if the session is in work state.
IP Address (ip_address)	IP address from which the session was initiated.
Last Login Time (last_login_time)	Session description.
Last Logout Time (last_logout_time)	Timestamp when user last accessed the management server.
Locks (locks)	Number of locked objects.
Phone Number (phone_number)	Administrator phone number.
Publish Time (publish_time)	Timestamp when user published changes on the management server.
Session Timeout (session_timeout)	Session expiration timeout in seconds.
State (state)	Session state.
Tags (tags)	Collection of tag objects identified by the name or UID. Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.
Username (user_name)	The name of the logged in user.
Workflow history (workflow_history)	Show details per each workflow action.
Workflow State (workflow_state)	Workflow session state.
Color (color)	Color of the object. Should be one of existing colors.
Comments (comments)	Comments string.
Domain (domain)	Information about the domain that holds the Object.
Icon (icon)	Object icon.
Meta Info (meta_info)	Object metadata.
Read Only (read_only)	Indicates whether the object is read-only.
Available Actions (available_actions)	Actions that are available on the object.

Checkpoint Management API/Assign Session method

Assign a session ownership to another administrator.

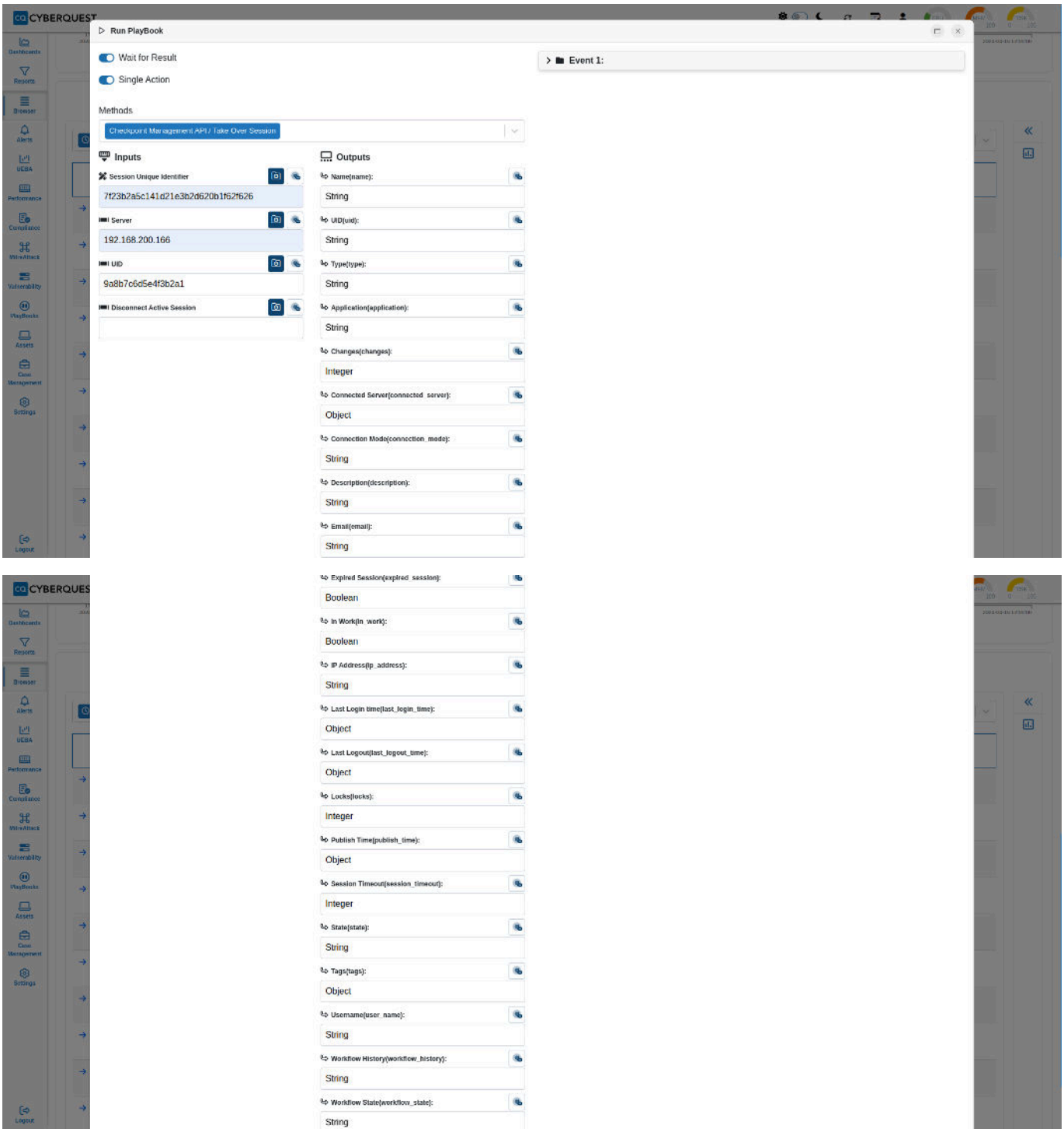


Inputs	Description
Session Unique Identifier (is required)	Session unique identifier as it returned by the login request
Server (is required)	Server Address
Administrator Name	Assignee administrator name. Specify it to assign a session to another administrator.
UID	Session unique identifier. Specify it to assign a different session than the one you currently use.
Disconnect Active Session	Allows assignment of an active session, currently executed by another administrator.

Outputs	Description
Message (message)	Operation status.

Checkpoint Management API/Take Over Session method

Take ownership of another session and start working on it.

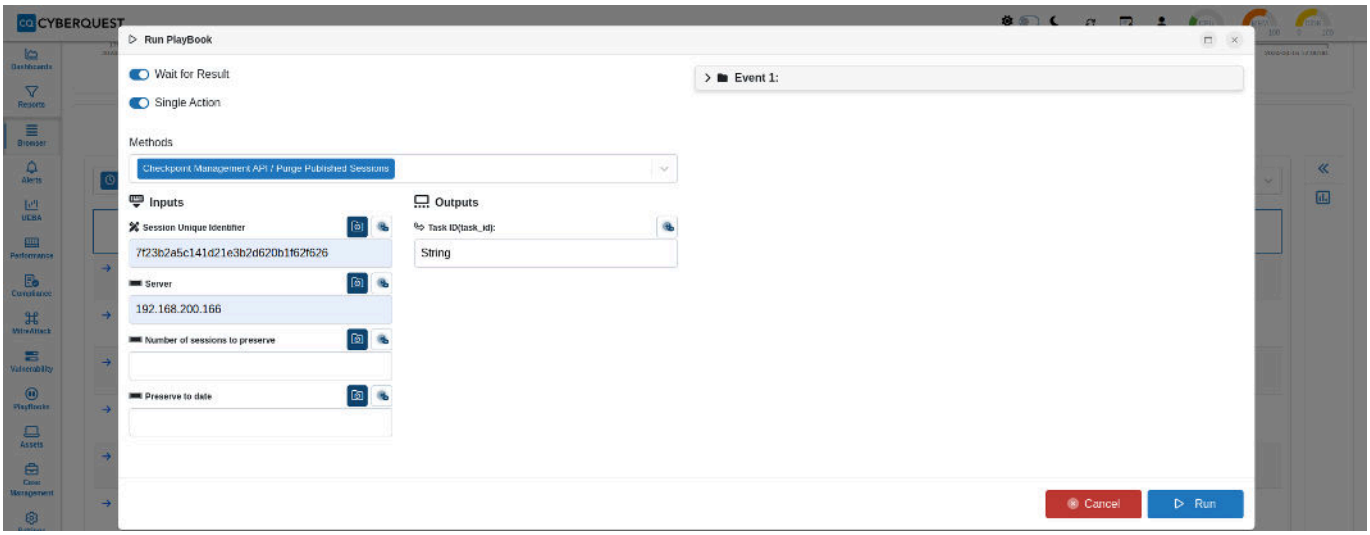


Inputs	Description
Session Unique Identifier (is required)	Session unique identifier as it returned by the login request
Server (is required)	Server Address
UID (is required)	Session unique identifier.
Disconnect Active Session	Allows taking over of an active session, currently executed by another administrator.

Outputs	Description
Name (name)	Object name. Must be unique in the domain.
UID (uid)	Object unique identifier.
Type (type)	Object type.
Application (application)	The name of the application serving the Management API requests.
Changes (changes)	Number of pending changes.
Connected Server (connected_server)	The server which the user is currently connected to.
Connection Mode (connection_mode)	Session connection mode.
Description (description)	Session description.
Email (email)	Administrator email.
Expired Session (expired_session)	True if the session is expired.
In Work (in_work)	True if the session is in work state.
IP Address (ip_address)	IP address from which the session was initiated.
Last Login time (last_login_time)	Session description.
Last Logout (last_logout_time)	Timestamp when user last accessed the management server.
Locks (locks)	Number of locked objects.
Publish Time (publish_time)	Timestamp when user published changes on the management server.
Session Timeout (session_timeout)	Session expiration timeout in seconds.
State (state)	Session state
Tags (tags)	Collection of tag objects identified by the name or UID. Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.
Username (user_name)	The name of the logged in user.
Workflow History (workflow_history)	Show details per each workflow action.
Workflow State (workflow_state)	Workflow session state.

Checkpoint Management API/Purge Published Sessions method

Permanently deletes all data which belongs to the published sessions not selected for preservation. This operation is irreversible.

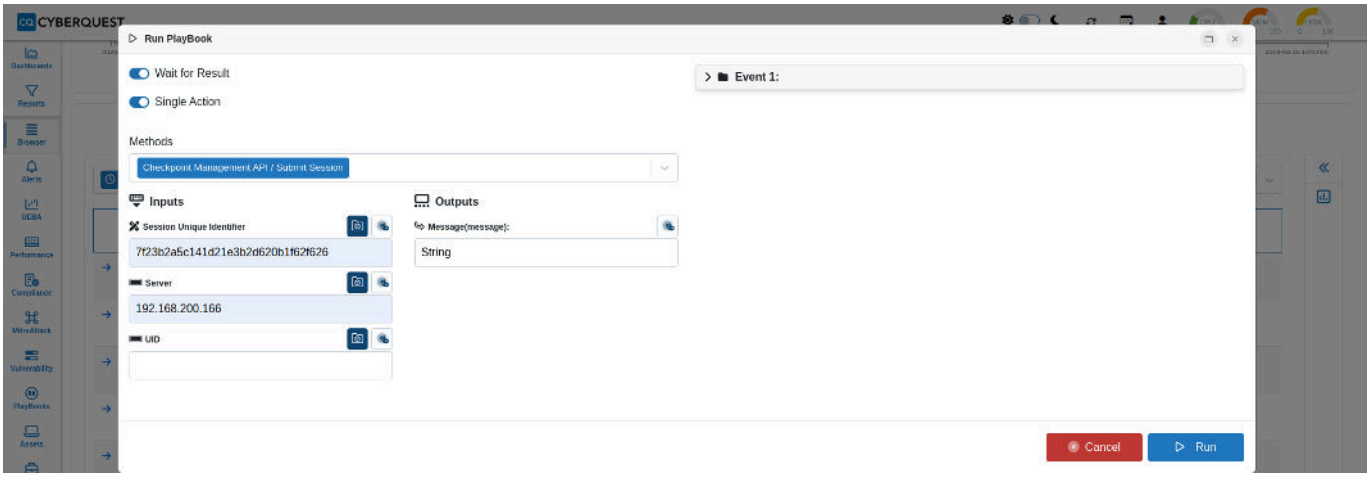


Inputs	Description
Session Unique Identifier (is required)	Session unique identifier as it returned by the login request
Server (is required)	Server Address
Number of sessions to preserve	The number of newest sessions to preserve, by the sessionss publish date. Number of sessions to preserve or Preserve to date is REQUIRED!
Preserve to date	The date until which sessions are preserved, by the sessionss publish date. ISO 8601. If timezone isnt specified in the input, the Management servers timezone is used. Number of sessions to preserve or Preserve to date is REQUIRED!

Outputs	Description
Task ID (task_id)	Asynchronous task unique identifier. Use show-task command to check the progress of the task.

Checkpoint Management API/Submit Session method

Workflow feature - Submit the session for approval.

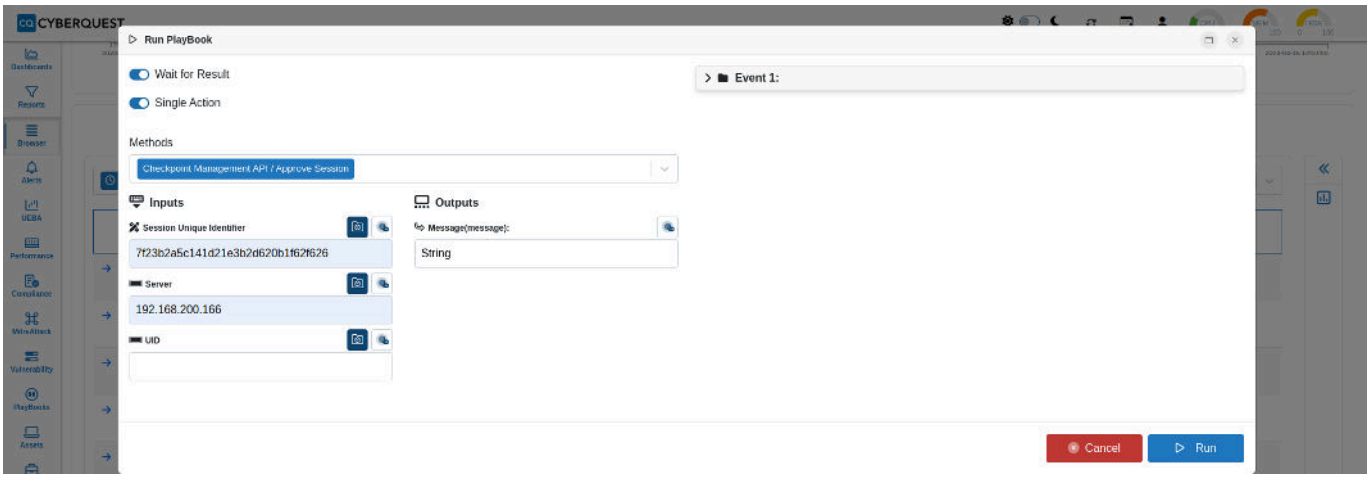


Inputs	Description
Session Unique Identifier (is required)	Session unique identifier as it returned by the login request
Server (is required)	Server Address
UID	Session unique identifier.

Outputs	Description
Message (message)	Operation status.

Checkpoint Management API/Approve Session method

Workflow feature - Approve and Publish the session.

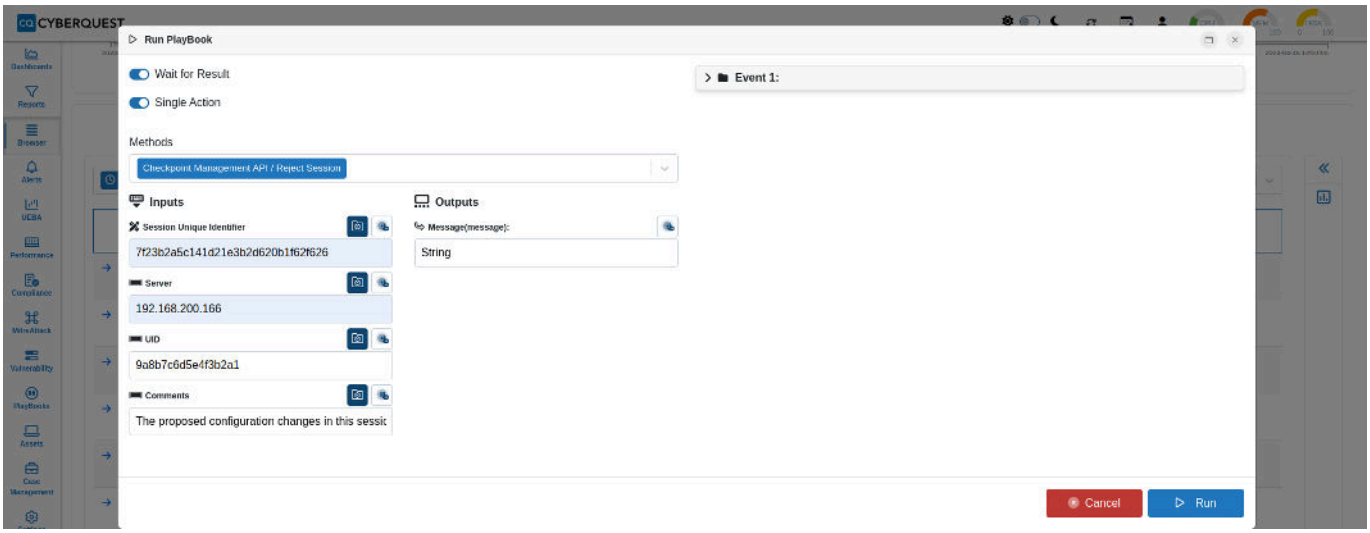


Inputs	Description
Session Unique Identifier (is required)	Session unique identifier as it returned by the login request
Server (is required)	Server Address
UID (is required)	Session unique identifier.

Outputs	Description
Message (message)	Operation status.

Checkpoint Management API/Reject Session method

Workflow feature - Return the session to the submitter administrator.

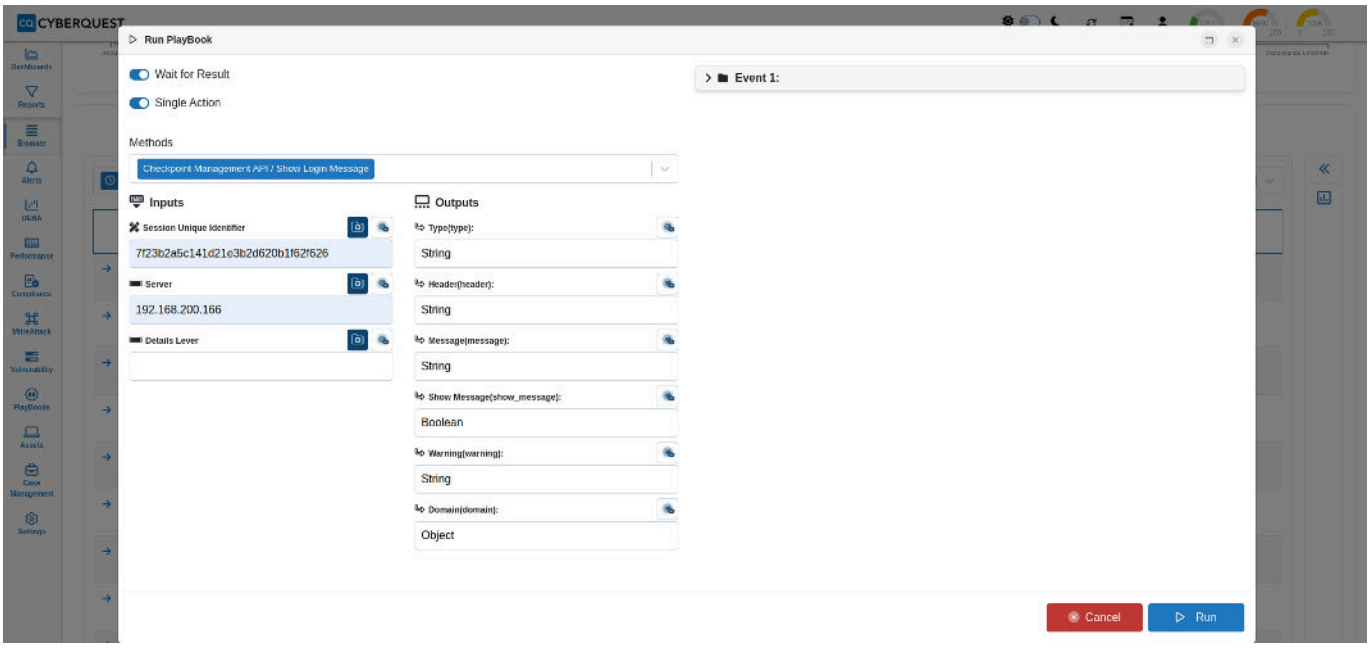


Inputs	Description
Session Unique Identifier (is required)	Session unique identifier as it returned by the login request
Server (is required)	Server Address
UID (is required)	Session unique identifier.
Comments (is required)	Reject justification.

Outputs	Description
Message (message)	Operation status.

Checkpoint Management API/Show Login Message method

Retrieve existing object using object name or uid.

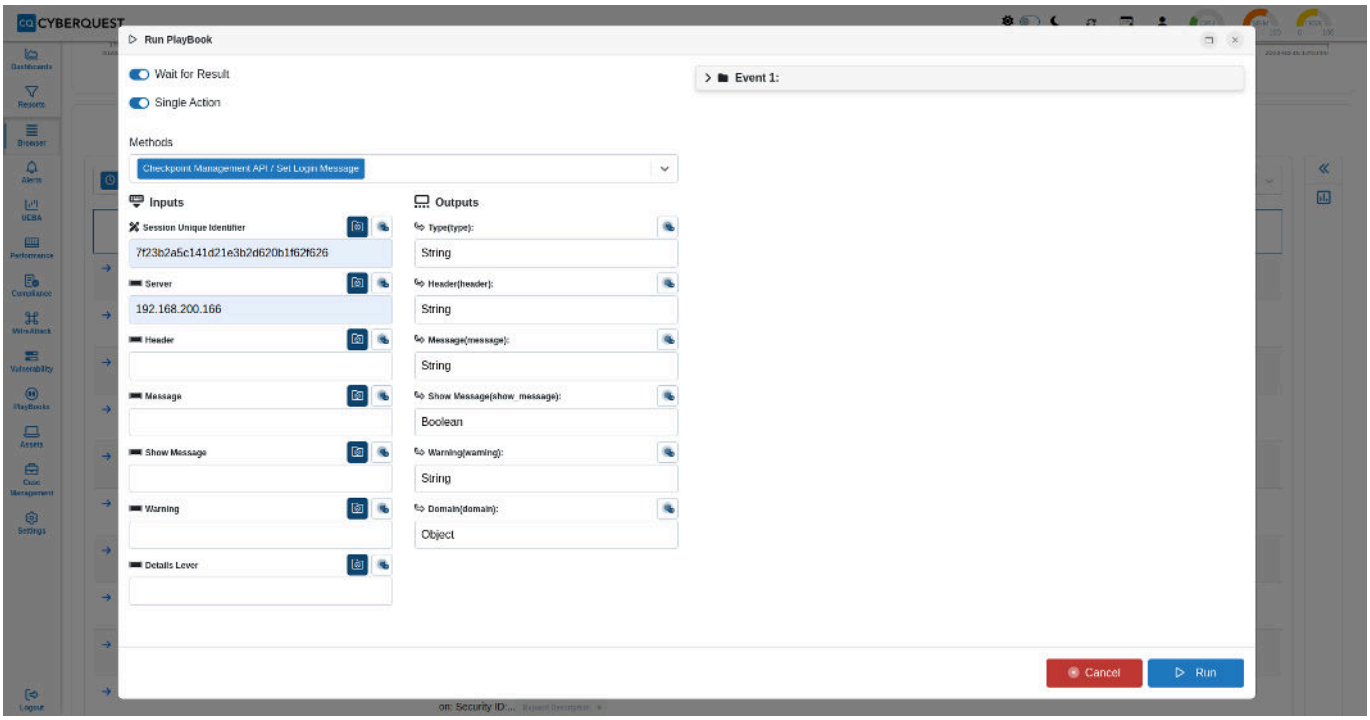


Inputs	Description
Session Unique Identifier (is required)	Session unique identifier as it returned by the login request
Server (is required)	Server Address
Details Lever	The level of detail for some of the fields in the response can vary from showing only the UID value of the object to a fully detailed representation of the object.

Outputs	Description
Type (type)	Object type.
Header (header)	Login message header
Message (message)	Login message body.
Show Message (show_message)	Whether to show login message.
Warning (warning)	Add warning sign.
Domain (domain)	Information about the domain that holds the Object.

Checkpoint Management API/Set Login Message method

Edit existing object using object name or uid.

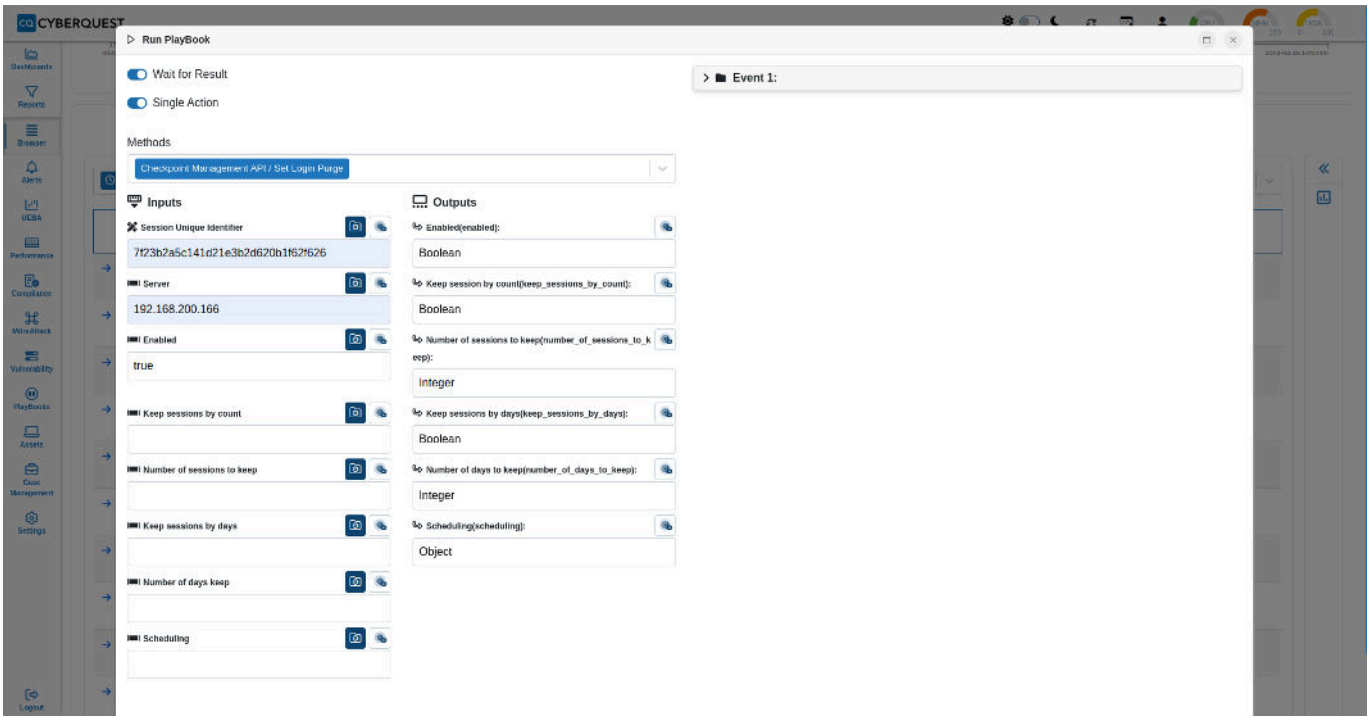


Inputs	Description
Session Unique Identifier (is required)	Session unique identifier as it returned by the login request
Server (is required)	Server Address
Header	Login message header.
Message	Login message body.
Show Message	Whether to show login message.
Warning	Add warning sign.
Details Lever	The level of detail for some of the fields in the response can vary from showing only the UID value of the object to a fully detailed representation of the object.

Outputs	Description
Type (type)	Object type.
Header (header)	Login message header
Message (message)	Login message body.
Show Message (show_message)	Whether to show login message.
Warning (warning)	Add warning sign.
Domain (domain)	Information about the domain that holds the Object

Checkpoint Management API/Set Login Purge method

Set Automatic Purge. NOTE! this command will permanently delete all of the data which belongs to the published sessions not selected for preservation. In Multi-Domain Server, it should be done for each domain.

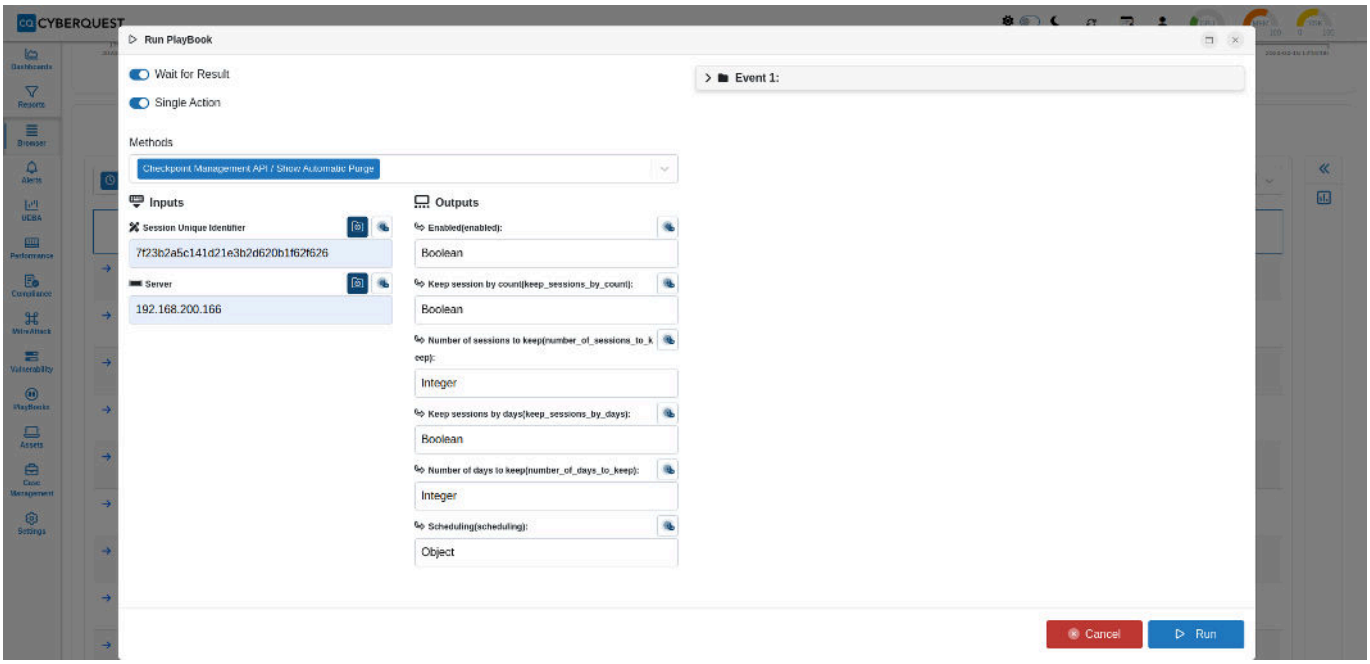


Inputs	Description
Session Unique Identifier (is required)	Session unique identifier as it returned by the login request
Server (is required)	Server Address
Enabled (is required)	Login message header.
Keep sessions by count	Whether or not to keep the latest N sessions. Note: when the automatic purge feature is enabled, this field and/or the keep-sessions-by-date field must be set to true.
Number of sessions to keep	When keep-sessions-by-count = true this sets the number of newest sessions to preserve, by the sessionss publish date.
Keep sessions by days	Whether or not to keep the sessions for D days. Note: when the automatic purge feature is enabled, this field and/or the keep-sessions-by-count field must be set to true.
Number of days keep	When keep-sessions-by-days = true this sets the number of days to keep the sessions.
Scheduling	When to purge sessions that do not meet the keep criteria. Note: when the automatic purge feature is enabled, this field must be set.

Outputs	Description
Enabled (enabled)	Turn on/off the automatic-purge feature.
Keep session by count (keep_sessions_by_count)	Whether or not to keep the latest N sessions.
Number of sessions to keep (number_of_sessions_to_keep)	The number of newest sessions to preserve, by the sessionss publish date.
Keep sessions by days (keep_sessions_by_days)	Whether or not to keep the sessions for D days.
Number of days to keep (number_of_days_to_keep)	When keep-sessions-by-days = true this sets the number of days to keep the sessions.
Scheduling (scheduling)	When to purge sessions that do not meet the keep criteria.

Checkpoint Management API/Show Automatic Purge method

Show Automatic Purge.

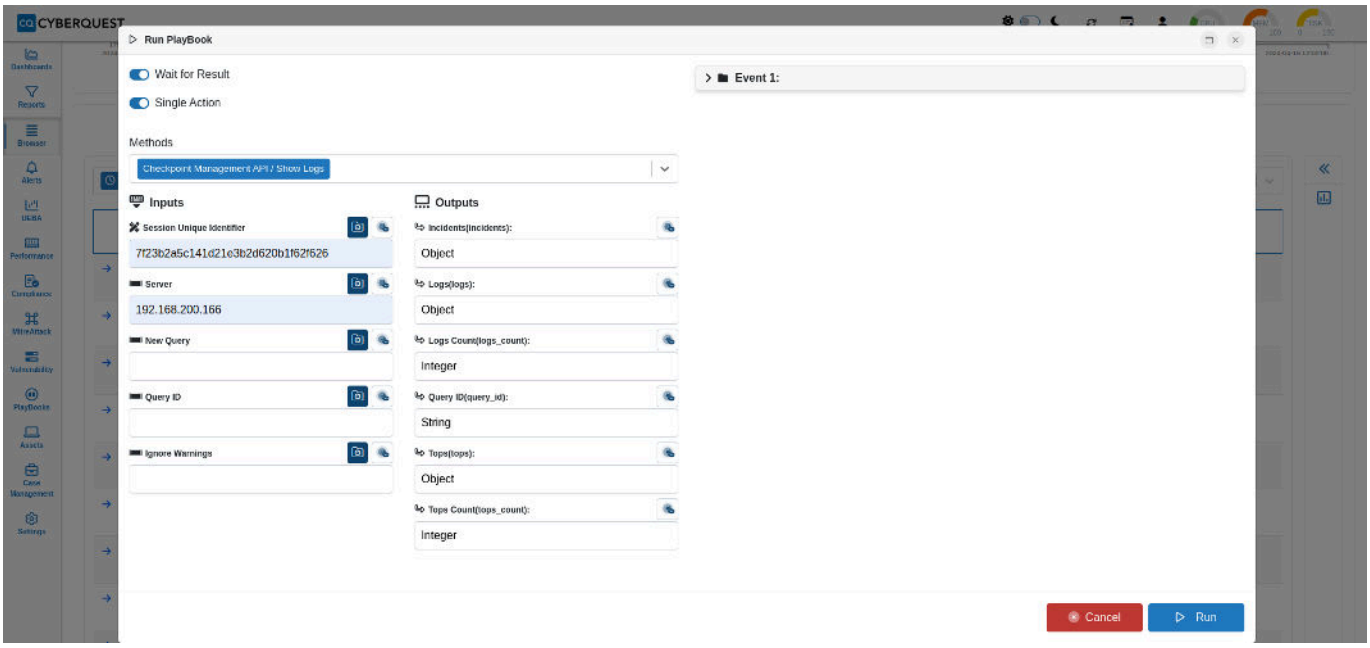


Inputs	Description
Session Unique Identifier (is required)	Session unique identifier as it returned by the login request
Server (is required)	Server Address

Outputs	Description
Enabled (enabled)	Turn on/off the automatic-purge feature.
Keep session by count (keep_sessions_by_count)	Whether or not to keep the latest N sessions.
Number of sessions to keep (number_of_sessions_to_keep)	The number of newest sessions to preserve, by the sessionss publish date.
Keep sessions by days (keep_sessions_by_days)	Whether or not to keep the sessions for D days.
Number of days to keep (number_of_days_to_keep)	When keep-sessions-by-days = true this sets the number of days to keep the sessions.
Scheduling (scheduling)	When to purge sessions that do not meet the keep criteria.

Checkpoint Management API/Show Logs method

Showing logs according to the given filter.

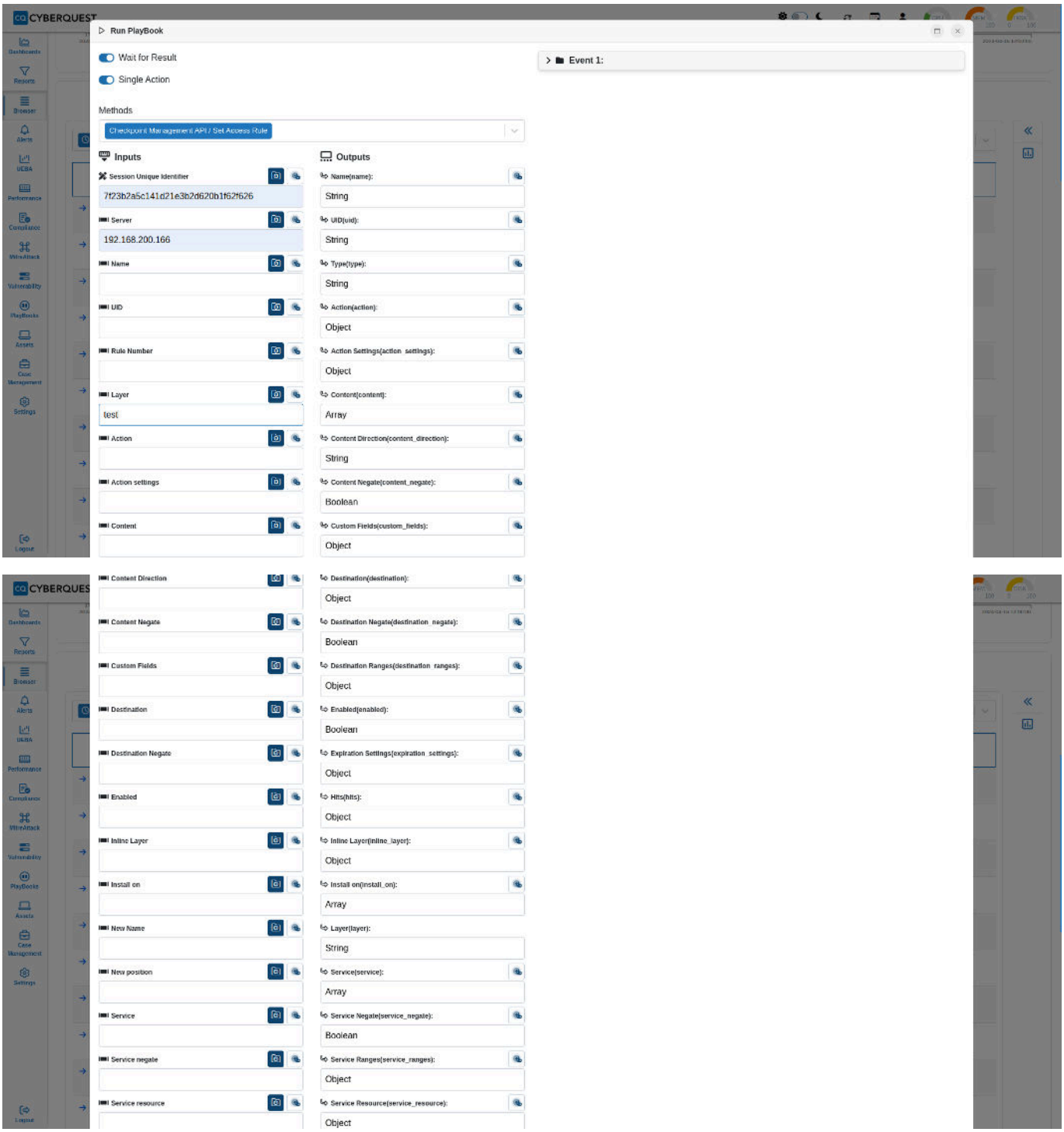


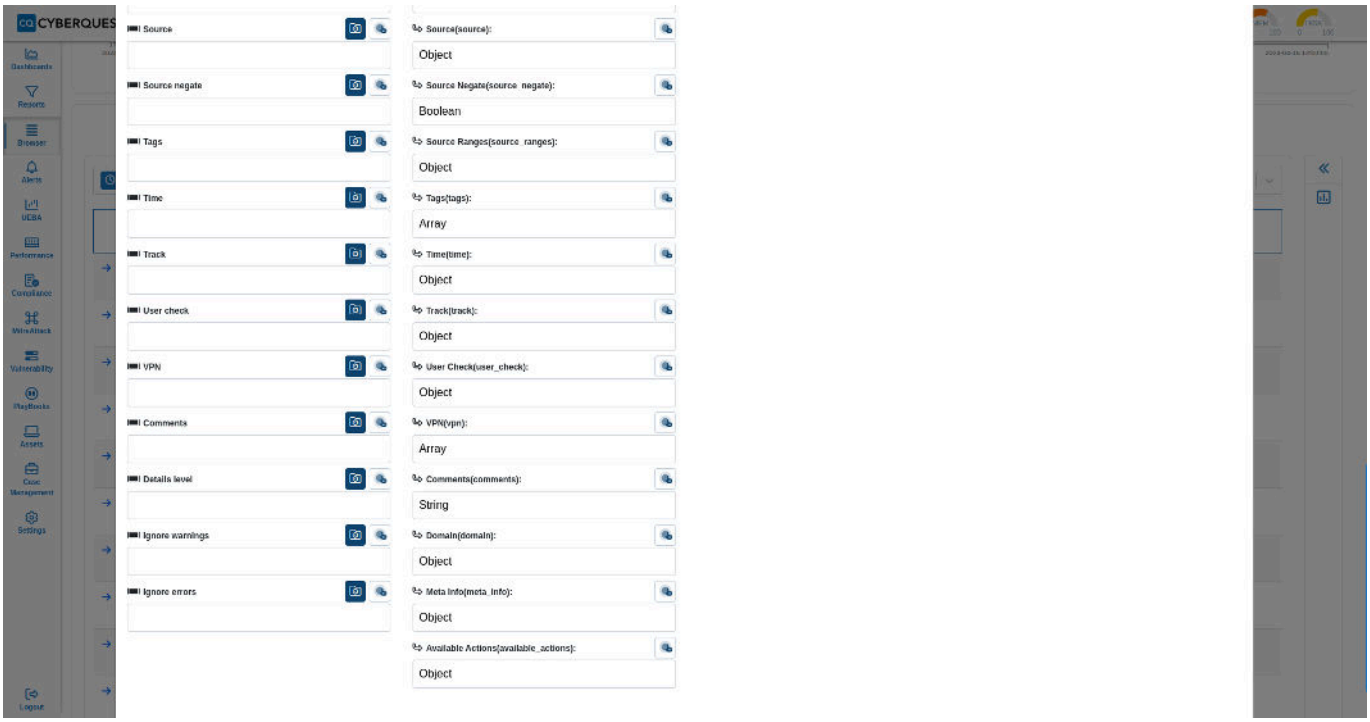
Inputs	Description
Session Unique Identifier (is required)	Session unique identifier as it returned by the login request
Server (is required)	Server Address
New Query	Running a new query.
Query ID	Get the next page of last run query with specified limit.
Ignore Warnings	Ignore warnings if exist

Outputs	Description
Incidents (incidents)	Incident object when error or warning occur.
Logs (logs)	Logs result.
Logs Count (logs_count)	Number of logs in the result.
Query ID (query_id)	Get the next page of last run query with specified limit.
Tops (tops)	Tops result.
Tops Count (tops_count)	Total logs in top response.

Checkpoint Management API/Set Access Rule method

Edit existing object using object name or uid.


CYBERQUEST
Run PlayBook
Wait for Result
Single Action
Methods
Checkpoint Management API / Set Access Rule
Inputs
Outputs
Event 1:
Session Unique Identifier
7f23b2a5c141d21e3b2d620b1f62f626
Server
192.168.200.166
Name
UID
Rule Number
Layer
test
Action
Action settings
Content
Content Direction
Content Negate
Custom Fields
Destination
Destination Negate
Enabled
Inline Layer
Install on
New Name
New position
Service
Service negate
Service resource
Name(name):
String
UID(uid):
String
Type(type):
String
Action(action):
Object
Action Settings(action_settings):
Object
Content(content):
Array
Content Direction(content_direction):
String
Content Negate(content_negate):
Boolean
Custom Fields(custom_fields):
Object
Destination(destination):
Object
Destination Negate(destination_negate):
Boolean
Destination Ranges(destination_ranges):
Object
Enabled(enabled):
Boolean
Expiration Settings(expiration_settings):
Object
Hits(hits):
Object
Inline Layer(inline_layer):
Object
Install on(install_on):
Array
Layer(layer):
String
Service(service):
Array
Service Negate(service_negate):
Boolean
Service Ranges(service_ranges):
Object
Service Resource(service_resource):
Object


Source
Source negate
Tags
Time
Track
User check
VPN
Comments
Details level
Ignore warnings
Ignore errors
Source(source):
Object
Source Negate(source_negate):
Boolean
Source Ranges(source_ranges):
Object
Tags(tags):
Array
Time(time):
Object
Track(track):
Object
User Check(user_check):
Object
VPN(vpn):
Array
Comments(comments):
String
Domain(domain):
Object
Meta Info(meta_info):
Object
Available Actions(available_actions):
Object

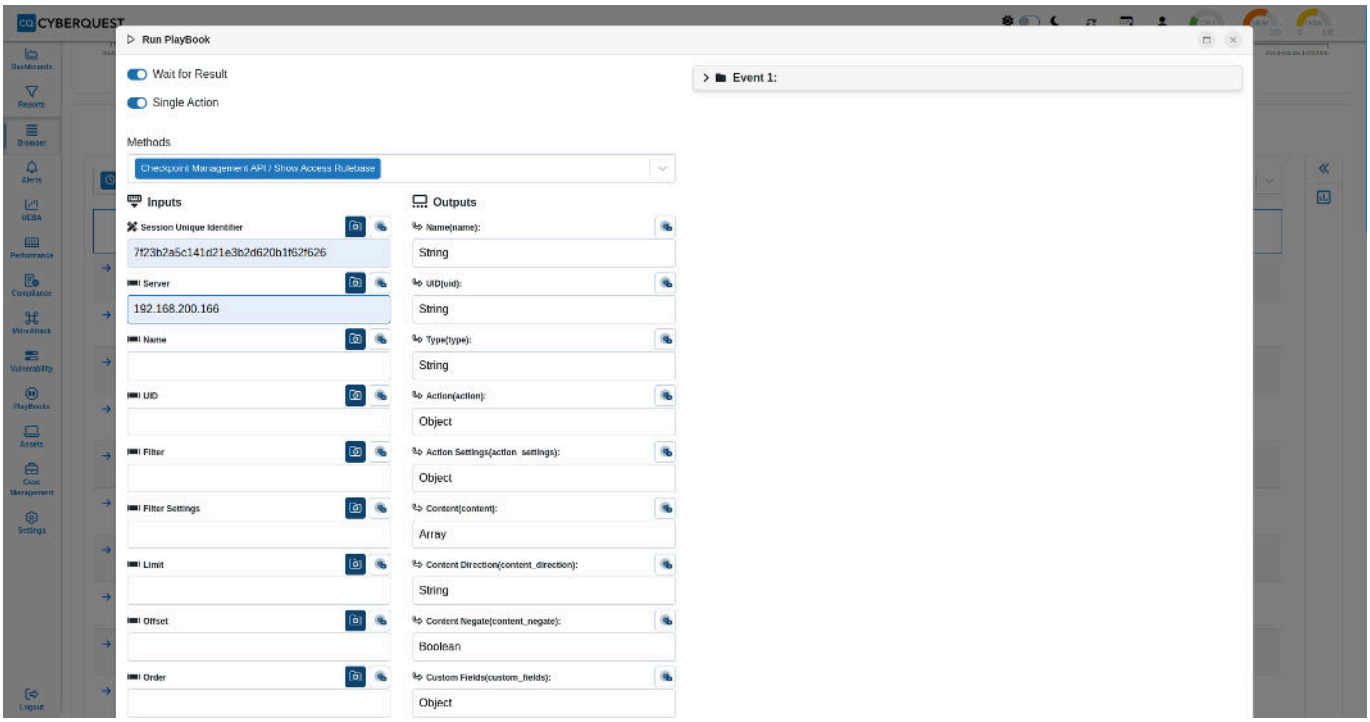
Inputs	Description
Session Unique Identifier (is required)	Session unique identifier as it returned by the login request
Server (is required)	Server Address
Name	Object name. Must be unique in the domain. Name or UID or Rule Number is REQUIRED!
UID	Object unique identifier. Name or UID or Rule Number is REQUIRED!
Rule Number	Rule number. Name or UID or Rule Number is REQUIRED!
Layer (is required)	Layer that the rule belongs to identified by the name or UID.
Action	Accept, Drop, Ask, Inform, Reject, User Auth, Client Auth, Apply Layer.
Action settings	Action settings.
Content	List of processed file types that this rule applies on.
Content Direction	On which direction the file types processing is applied.
Content Negate	True if negate is set for data.
Custom Fields	Custom fields.
Destination	Collection of Network objects identified by the name or UID.
Destination Negate	True if negate is set for destination.
Enabled	Enable/Disable the rule.
Inline Layer	Inline Layer identified by the name or UID. Relevant only if Action was set to Apply Layer.
Install on	Which Gateways identified by the name or UID to install the policy on.
New Name	The level of detail for some of the fields in the response can vary from showing only the UID value of the object to a fully detailed representation of the object.
New position	New position in the rulebase.
Service	Collection of Network objects identified by the name or UID.
Service negate	True if negate is set for service.
Service resource	Resource of the service identified by the name or UID. When a service-resource exists, the service parameter should contains exactly one service element.
Source	Collection of Network objects identified by the name or UID.
Source negate	True if negate is set for source.
Tags	Collection of tag objects identified by the name or UID.
Time	List of time objects. For example: Weekend, Off-Work, Every-Day.
Track	Track Settings.
User check	UserCheck settings.
VPN	Communities or Directional.
Comments	Comments string.
Details level	The level of detail for some of the fields in the response can vary from showing only the UID value of the object to a fully detailed representation of the object.
Ignore warnings	Apply changes ignoring warnings.
Ignore errors	Apply changes ignoring errors. You wont be able to publish such a changes. If ignore-warnings flag was omitted - warnings will also be ignored.

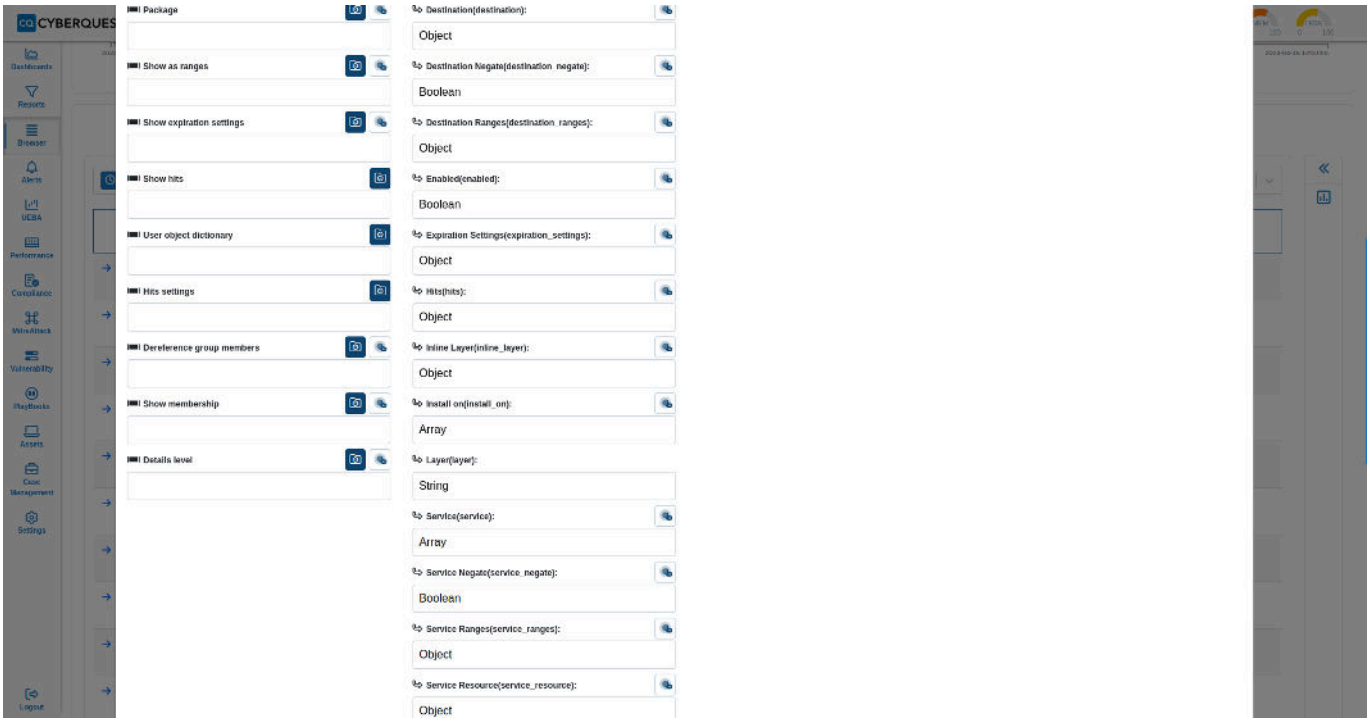
Outputs	Description
Name (name)	Object name. Must be unique in the domain.
UID (uid)	Object unique identifier.
Type (type)	Object type.
Action (action)	Accept, Drop, Ask, Inform, Reject, User Auth, Client Auth, Apply Layer. Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.
Action Settings (action_settings)	Action settings.
Content (content)	Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.
Content Direction (content_direction)	On which direction the file types processing is applied.
Content Negate (content_negate)	True if negate is set for data.
Custom Fields (custom_fields)	Custom fields.
Destination (destination)	Collection of Network objects identified by the name or UID. Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.
Destination Negate (destination_negate)	True if negate is set for destination.
Destination Ranges (destination_ranges)	Displays the destination as ranges of IP addresses, in case show-as-ranges is set to true.In this case, destination and destination-negate parameters are omitted.
Enabled (enabled)	Enable/Disable the rule.
Expiration Settings (expiration_settings)	Displays the expiration date settings.
Hits (hits)	Hits count object.
Inline Layer (inline_layer)	Inline Layer identified by the name or UID. Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.
Install on (install_on)	Which gateway, identified by the name or UID, to install the policy. Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.
Layer (layer)	
Service (service)	Collection of Network objects identified by the name or UID. Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.
Service Negate (service_negate)	True if negate is set for service.
Service Ranges (service_ranges)	Displays the services and applications as ranges of port numbers, in case show-as-ranges is set to true.In this case, service and service-negate parameters are omitted.
Service Resource (service_resource)	Resource of the service.
Source (source)	Collection of Network objects identified by the name or UID. Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.
Source Negate (source_negate)	True if negate is set for source.

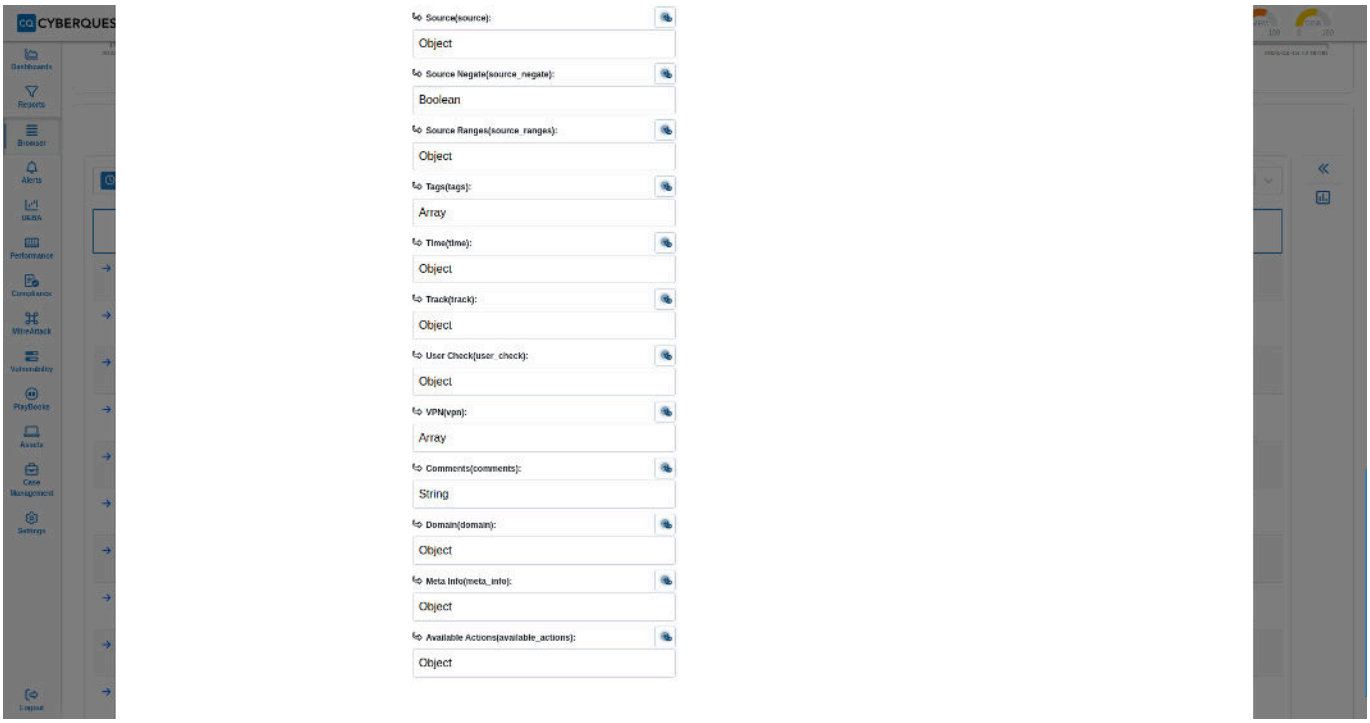
Outputs	Description
Source Ranges (source_ranges)	Displays the source as ranges of IP addresses, in case show-as-ranges is set to true.In this case, source and source-negate parameters are omitted.
Tags (tags)	Collection of tag objects identified by the name or UID
Time (time)	List of time objects. For example: Weekend, Off-Work, Every-Day. Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.
Track (track)	Track Settings.
User Check (user_check)	UserCheck settings.
VPN (vpn)	VPN settings. Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.
Comments (comments)	Comments string.
Domain (domain)	Information about the domain that holds the Object.
Meta Info (meta_info)	Object metadata.
Available Actions (available_actions)	Actions that are available on the object.

Checkpoint Management API/Show Access Rulebase method

Shows the entire Access Rules layer. This layer is divided into sections. An Access Rule may be within a section, or independent of a section (in which case it is said to be under the global section). The reply features a list of objects. Each object may be a section of the layer, with all its rules in, or a rule itself, for the case of rules which are under the global section. An optional filter field may be added in order to filter out only those rules that match a search criteria.




Package
Show as ranges
Show expiration settings
Show hits
User object dictionary
Hits settings
Dereference group members
Show membership
Details level
Destination(destination):
Object
Destination Negate(destination_negate):
Boolean
Destination Ranges(destination_ranges):
Object
Enabled(enabled):
Boolean
Expiration Settings(expiration_settings):
Object
Hits(hits):
Object
Inline Layer(inline_layer):
Object
Install on(install_on):
Array
Layer(layer):
String
Service(service):
Array
Service Negate(service_negate):
Boolean
Service Ranges(service_ranges):
Object
Service Resource(service_resource):
Object


Source(source):
Object
Source Negate(source_negate):
Boolean
Source Ranges(source_ranges):
Object
Tags(tags):
Array
Time(time):
Object
Track(track):
Object
User Check(user_check):
Object
VPN(vpn):
Array
Comments(comments):
String
Domain(domain):
Object
Meta Info(meta_info):
Object
Available Actions(available_actions):
Object

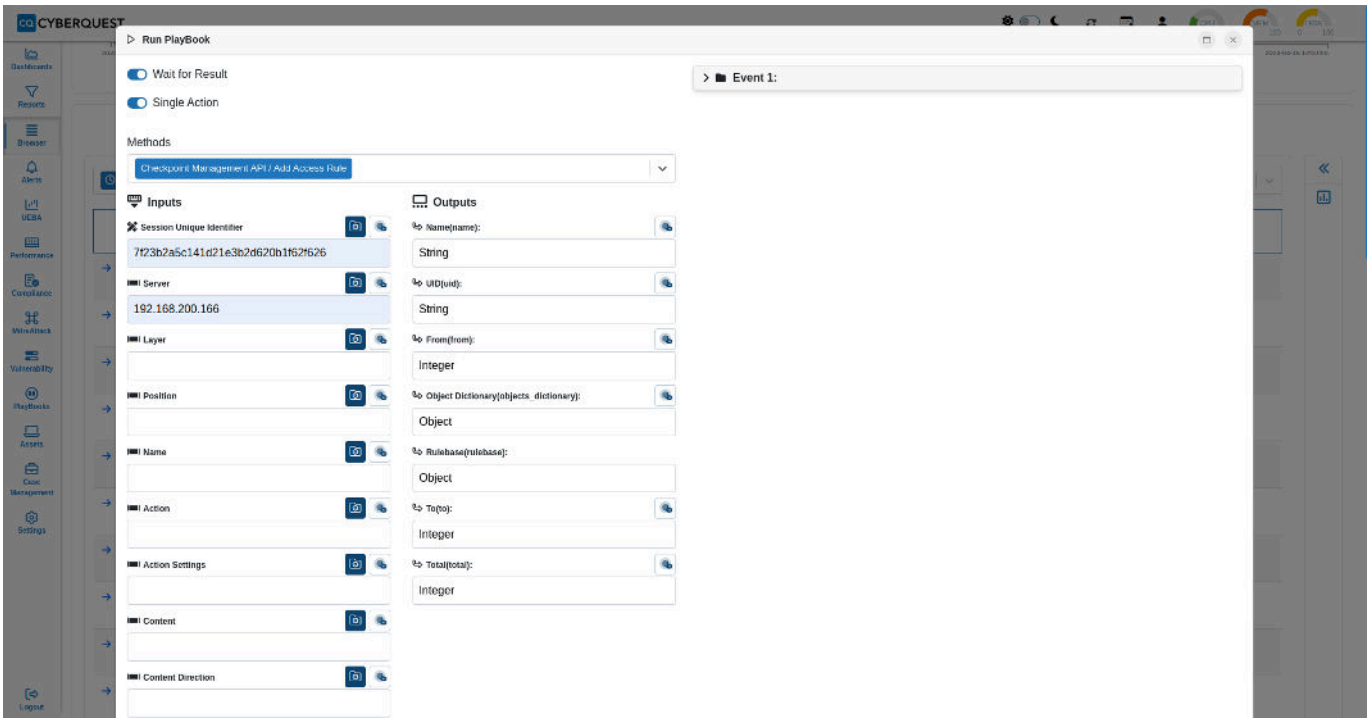
Inputs	Description
Session Unique Identifier (is required)	Session unique identifier as it returned by the login request
Server (is required)	Server Address
Name	Object name. Must be unique in the domain. Name or UID is REQUIRED!
UID	Object unique identifier. Name or UID is REQUIRED!
Filter	Search expression to filter the rulebase. The provided text should be exactly the same as it would be given in Smart Console. The logical operators in the expression (AND, OR) should be provided in capital letters. If an operator is not used, the default OR operator applies.
Filter Settings	Sets filter preferences.
Limit	The maximal number of returned results.
Offset	Number of the results to initially skip.
Order	Sorts the results by search criteria. Automatically sorts the results by Name, in the ascending order.
Package	Name of the package.
Show as ranges	When true, the source, destination and services & applications parameters are displayed as ranges of IP addresses and port numbers rather than network objects.Objects that are not represented using IP addresses or port numbers are presented as objects.In addition, the response of each rule does not contain the parameters: source, source-negate, destination, destination-negate, service and service-negate, but instead it contains the parameters: source-ranges, destination-ranges and service-ranges.Note: Requesting to show rules as ranges is limited up to 20 rules per request, otherwise an error is returned. If you wish to request more rules, use the offset and limit parameters to limit your request.
Show expiration settings	Indicates whether to calculate and show expiration date settings field in reply.
Show hits	
User object dictionary	
Hits settings	
Dereference group members	Indicates whether to dereference members field by details level for every object in reply.
Show membership	Indicates whether to calculate and show groups field for every object in reply.
Details level	The level of detail for some of the fields in the response can vary from showing only the UID value of the object to a fully detailed representation of the object.

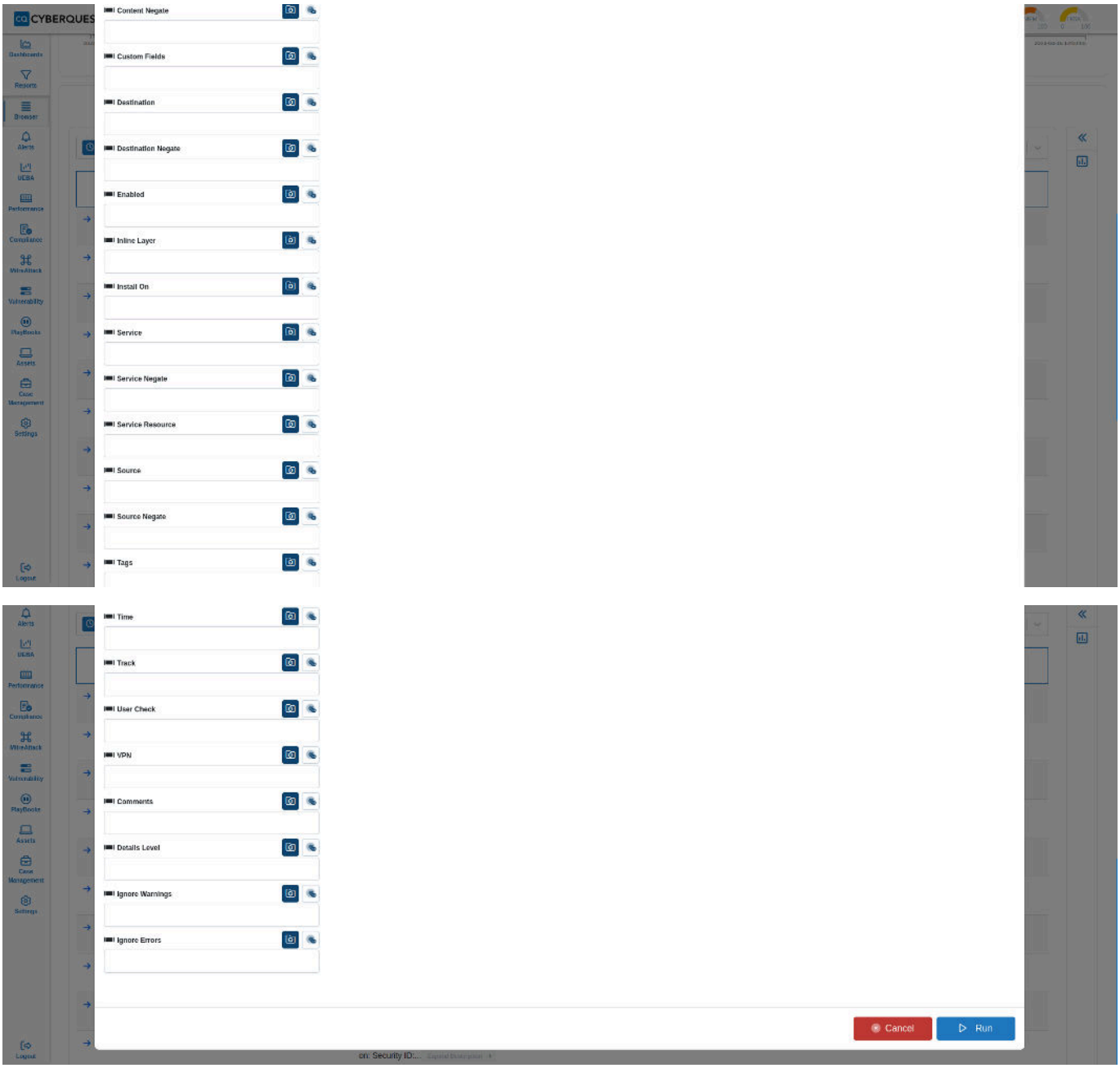
Outputs	Description
Name (name)	Object name. Must be unique in the domain.
UID (uid)	Object unique identifier.
Type (type)	Object type.
Action (action)	Accept, Drop, Ask, Inform, Reject, User Auth, Client Auth, Apply Layer. Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.
Action Settings (action_settings)	Action settings.
Content (content)	Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.
Content Direction (content_direction)	On which direction the file types processing is applied.
Content Negate (content_negate)	True if negate is set for data.
Custom Fields (custom_fields)	Custom fields.
Destination (destination)	Collection of Network objects identified by the name or UID. Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.
Destination Negate (destination_negate)	True if negate is set for destination.
Destination Ranges (destination_ranges)	Displays the destination as ranges of IP addresses, in case show-as-ranges is set to true.In this case, destination and destination-negate parameters are omitted.
Enabled (enabled)	Enable/Disable the rule.
Expiration Settings (expiration_settings)	Displays the expiration date settings.
Hits (hits)	Hits count object.
Inline Layer (inline_layer)	Inline Layer identified by the name or UID. Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.
Install on (install_on)	Which gateway, identified by the name or UID, to install the policy. Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.
Layer (layer)	
Service (service)	Collection of Network objects identified by the name or UID. Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.
Service Negate (service_negate)	True if negate is set for service.
Service Ranges (service_ranges)	Displays the services and applications as ranges of port numbers, in case show-as-ranges is set to true.In this case, service and service-negate parameters are omitted.
Service Resource (service_resource)	Resource of the service.
Source (source)	Collection of Network objects identified by the name or UID. Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.
Source Negate (source_negate)	True if negate is set for source.

Outputs	Description
Source Ranges (source_ranges)	Displays the source as ranges of IP addresses, in case show-as-ranges is set to true.In this case, source and source-negate parameters are omitted.
Tags (tags)	Collection of tag objects identified by the name or UID
Time (time)	List of time objects. For example: Weekend, Off-Work, Every-Day. Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.
Track (track)	Track Settings.
User Check (user_check)	UserCheck settings.
VPN (vpn)	VPN settings. Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.
Comments (comments)	Comments string.
Domain (domain)	Information about the domain that holds the Object.
Meta Info (meta_info)	Object metadata.
Available Actions (available_actions)	Actions that are available on the object.

Checkpoint Management API/Add Access Rule method

Create new object.



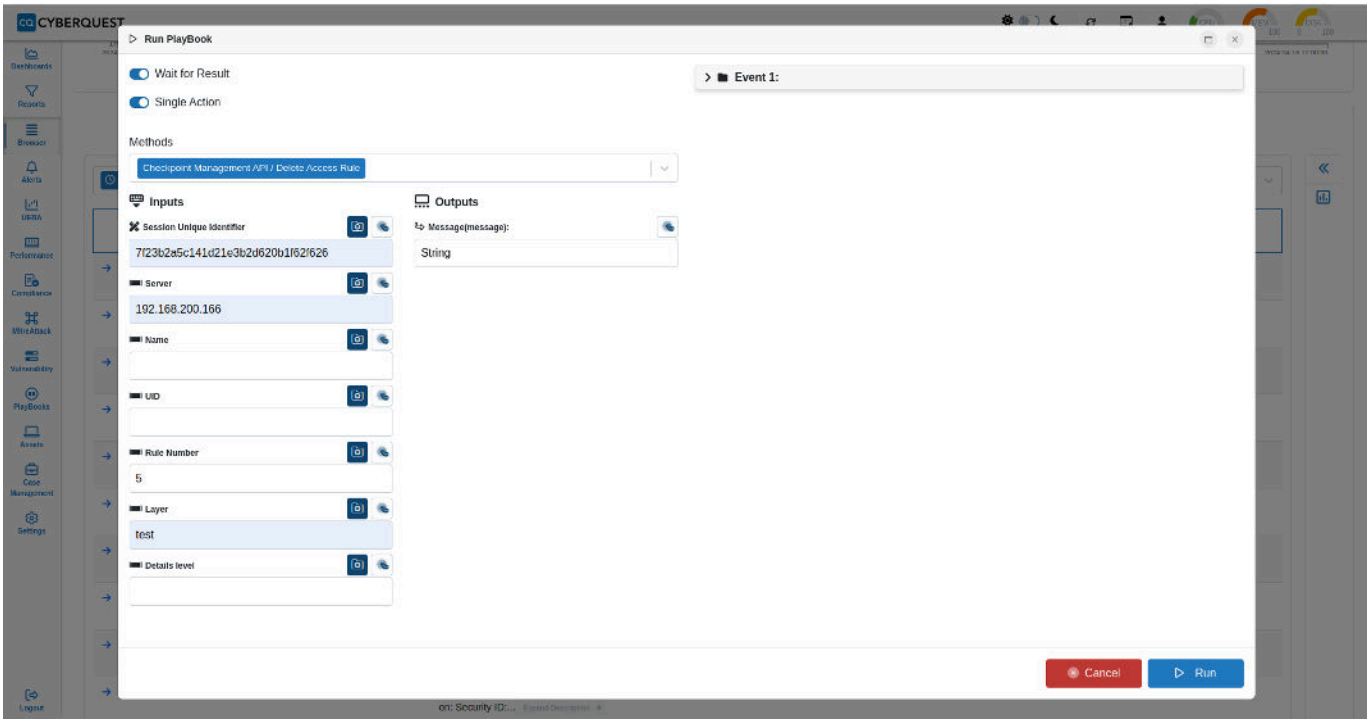

Content Negate
Custom Fields
Destination
Destination Negate
Enabled
Inline Layer
Install On
Service
Service Negate
Service Resource
Source
Source Negate
Tags
Time
Track
User Check
VPN
Comments
Details Level
Ignore Warnings
Ignore Errors
Cancel
Run

Inputs	Description
Session Unique Identifier (is required)	Session unique identifier as it returned by the login request
Server (is required)	Server Address
Layer	Layer that the rule belongs to identified by the name or UID.
Position	Position in the rulebase.
Name	Rule name.
Action	Accept, Drop, Ask, Inform, Reject, User Auth, Client Auth, Apply Layer
Action Settings	Action settings.
Content	List of processed file types that this rule applies on.
Content Direction	On which direction the file types processing is applied.
Content Negate	True if negate is set for data.
Custom Fields	Custom fields.
Destination	Collection of Network objects identified by the name or UID.
Destination Negate	True if negate is set for destination.
Enabled	Enable/Disable the rule.
Inline Layer	Inline Layer identified by the name or UID. Relevant only if Action was set to Apply Layer
Install On	Which Gateways identified by the name or UID to install the policy on.
Service	Collection of Network objects identified by the name or UID.
Service Negate	True if negate is set for service.
Service Resource	Resource of the service identified by the name or UID. When a service-resource exists, the service parameter should contains exactly one service element.
Source	Collection of Network objects identified by the name or UID.
Source Negate	True if negate is set for source.
Tags	Collection of tag objects identified by the name or UID.
Time	List of time objects. For example: Weekend, Off-Work, Every-Day.
Track	Track Settings.
User Check	UserCheck settings.
VPN	Communities or Directional.
Comments	Comments string.
Details Level	The level of detail for some of the fields in the response can vary from showing only the UID value of the object to a fully detailed representation of the object.
Ignore Warnings	Apply changes ignoring warnings.
Ignore Errors	Apply changes ignoring errors. You wont be able to publish such a changes. If ignore-warnings flag was omitted - warnings will also be ignored.

Outputs	Description
Name (name)	Object name. Must be unique in the domain.
UID (uid)	Object unique identifier.
From (from)	From which element number the query was done.
Object Dictionary (objects_dictionary)	Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.
Rulebase (rulebase)	
To (to)	To which element number the query was done.
Total (total)	Total number of elements returned by the query.

Checkpoint Management API/Delete Access Rule method

Delete existing object using object name or uid.

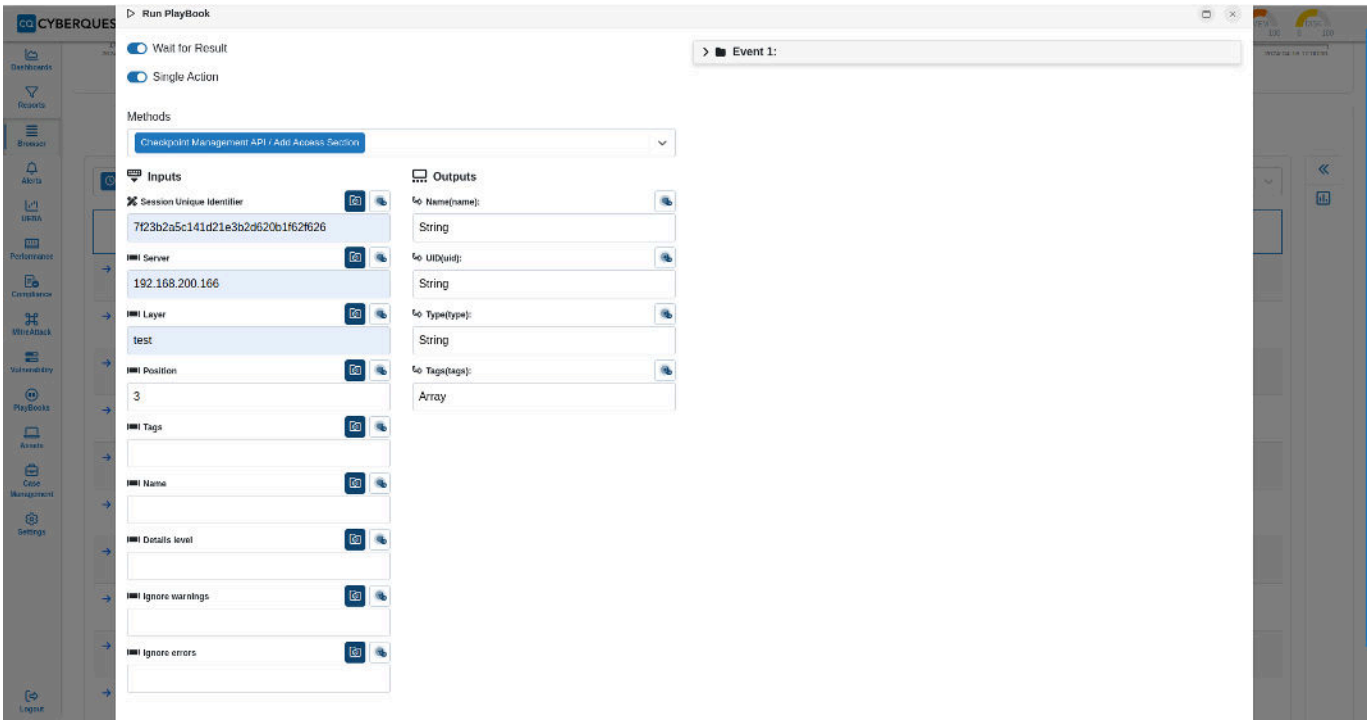


Inputs	Description
Session Unique Identifier (is required)	Session unique identifier as it returned by the login request
Server (is required)	Server Address
Name	Object name.
UID	Object unique identifier.
Rule Number (is required)	Rule number.
Layer (is required)	Layer that the rule belongs to identified by the name or UID.
Details level	The level of detail for some of the fields in the response can vary from showing only the UID value of the object to a fully detailed representation of the object.

Outputs	Description
Message (message)	Object name. Must be unique in the domain.

Checkpoint Management API/Add Access Section method

Create new object.

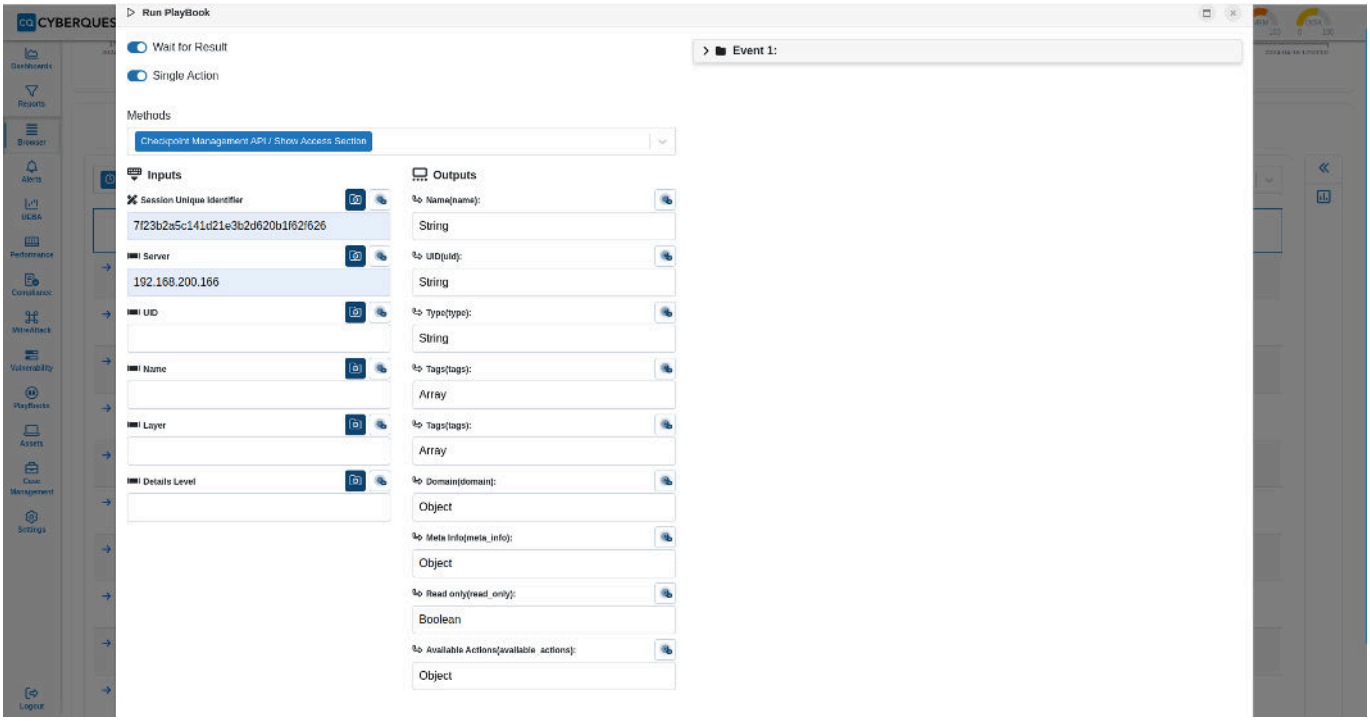


Inputs	Description
Session Unique Identifier (is required)	Session unique identifier as it returned by the login request
Server (is required)	Server Address
Layer (is required)	Layer that the rule belongs to identified by the name or UID.
Position (is required)	Position in the rulebase
Tags	Collection of tag objects identified by the name or UID.
Name	Object name. Must be unique in the domain.
Details level	The level of detail for some of the fields in the response can vary from showing only the UID value of the object to a fully detailed representation of the object.
Ignore warnings	Apply changes ignoring warnings.
Ignore errors	Apply changes ignoring errors. You wont be able to publish such a changes. If ignore-warnings flag was omitted - warnings will also be ignored.

Outputs	Description
Name (name)	Object name. Must be unique in the domain.
UID (uid)	Object unique identifier.
Type (type)	Object type.
Tags (tags)	Collection of tag objects identified by the name or UID. Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.

Checkpoint Management API/Show Access Section method

Retrieve existing object using object name or uid.

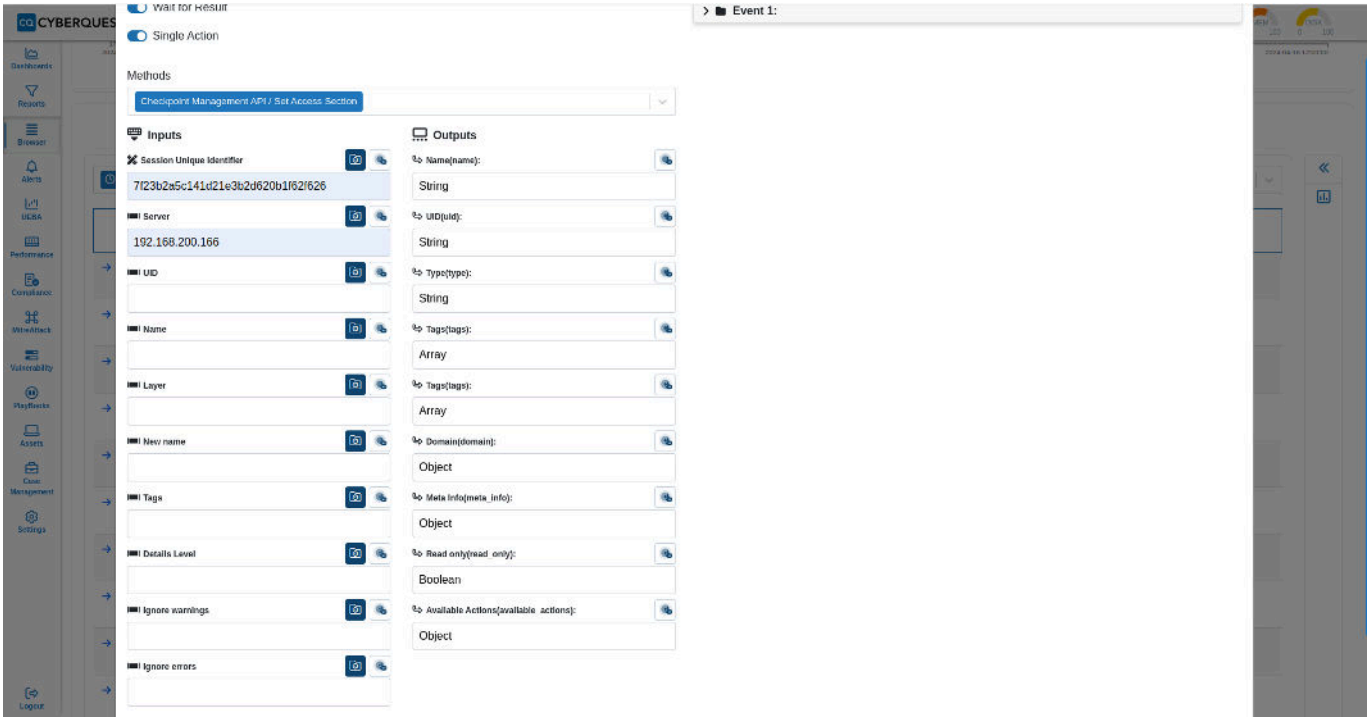


Inputs	Description
Session Unique Identifier (is required)	Session unique identifier as it returned by the login request
Server (is required)	Server Address
UID	Object unique identifier. UID or Name REQUIRED
Name	Object name. UID or Name REQUIRED
Layer (is required)	Layer that the rule belongs to identified by the name or UID.
Details Level	The level of detail for some of the fields in the response can vary from showing only the UID value of the object to a fully detailed representation of the object.

Outputs	Description
Name (name)	Object name. Must be unique in the domain.
UID (uid)	Object unique identifier.
Type (type)	Object type.
Tags (tags)	Collection of tag objects identified by the name or UID. Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.
Tags (tags)	Collection of tag objects identified by the name or UID. Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.
Domain (domain)	Information about the domain that holds the Object.
Meta Info (meta_info)	Object metadata.
Read only (read_only)	Indicates whether the object is read-only.
Available Actions (available_actions)	Actions that are available on the object.

Checkpoint Management API/Set Access Section method

Edit existing object using object name or uid.

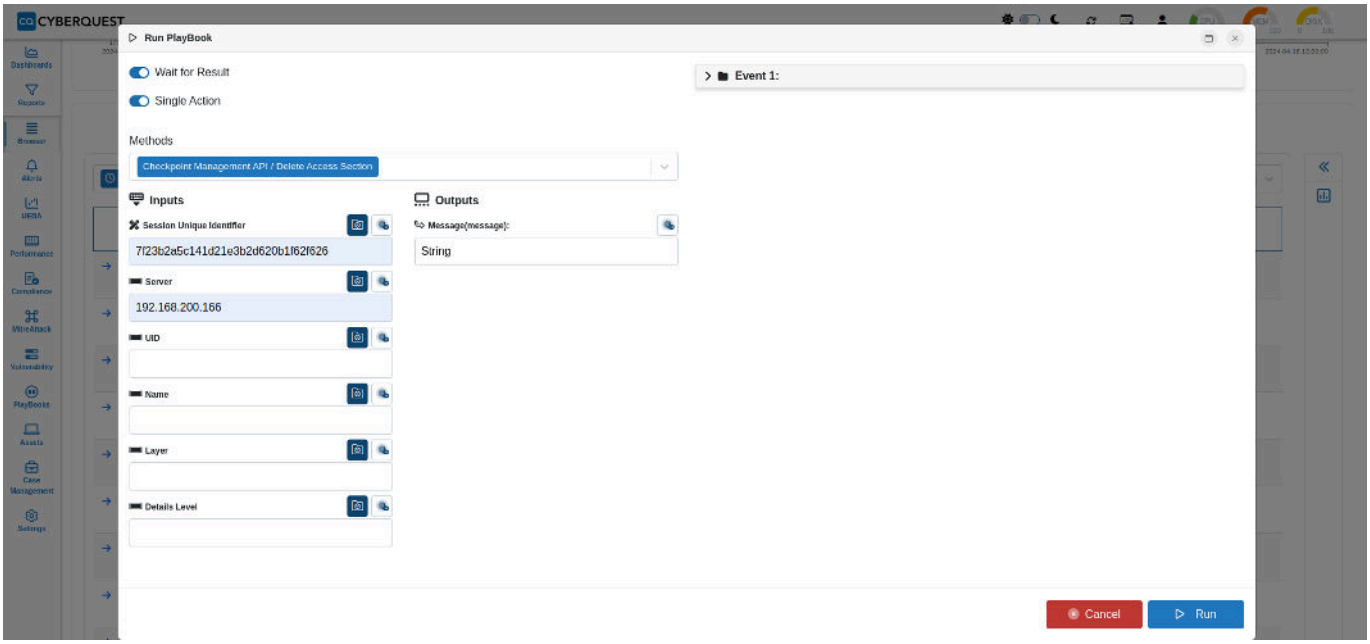


Inputs	Description
Session Unique Identifier (is required)	Session unique identifier as it returned by the login request
Server (is required)	Server Address
UID	Object unique identifier. UID or Name REQUIRED
Name	Object name. UID or Name REQUIRED
Layer (is required)	Layer that the rule belongs to identified by the name or UID.
New name	New name of the object.
Tags	Collection of tag objects identified by the name or UID.
Details Level	The level of detail for some of the fields in the response can vary from showing only the UID value of the object to a fully detailed representation of the object.
Ignore warnings	Apply changes ignoring warnings.
Ignore errors	Apply changes ignoring errors. You wont be able to publish such a changes. If ignore-warnings flag was omitted - warnings will also be ignored.

Outputs	Description
Name (name)	Object name. Must be unique in the domain.
UID (uid)	Object unique identifier.
Type (type)	Object type.
Tags (tags)	Collection of tag objects identified by the name or UID. Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.
Tags (tags)	Collection of tag objects identified by the name or UID. Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.
Domain (domain)	Information about the domain that holds the Object.
Meta Info (meta_info)	Object metadata.
Read only (read_only)	Indicates whether the object is read-only.
Available Actions (available_actions)	Actions that are available on the object.

Checkpoint Management API/Delete Access Section method

Delete existing object using object name or uid.

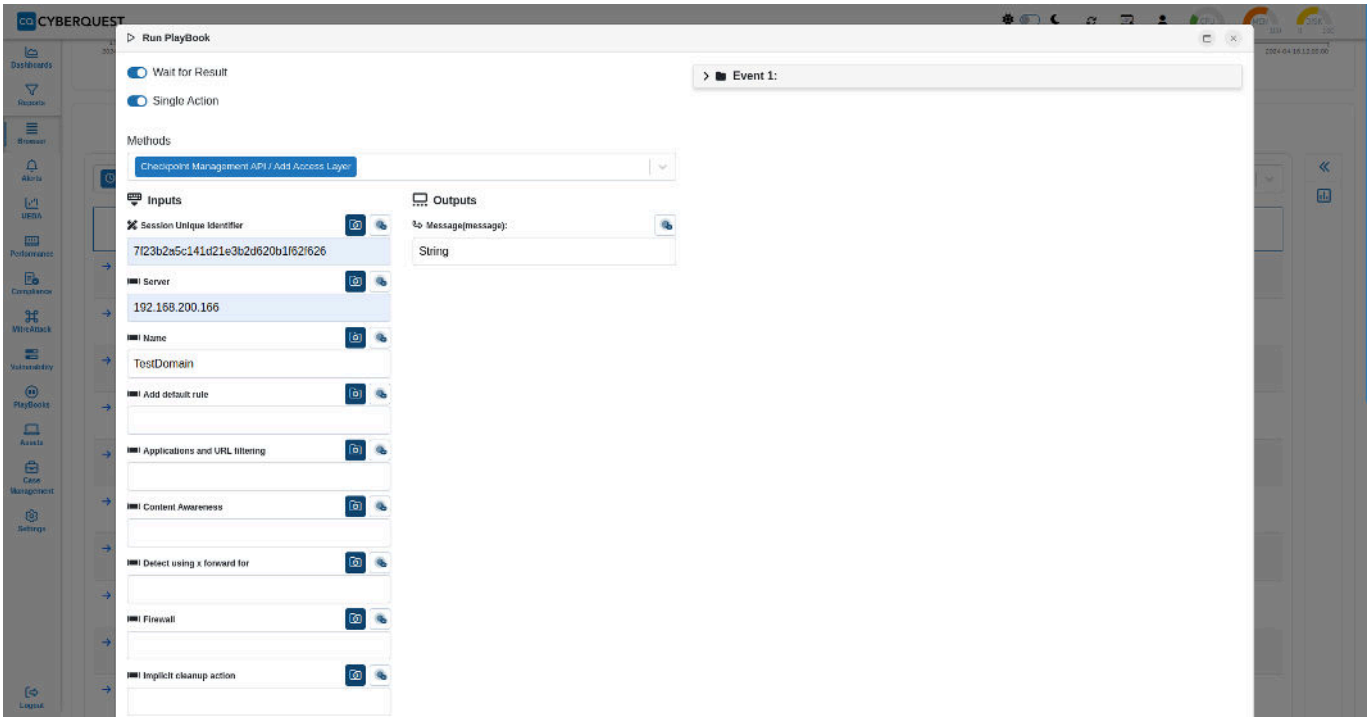


Inputs	Description
Session Unique Identifier (is required)	Session unique identifier as it returned by the login request
Server (is required)	Server Address
UID	Object unique identifier. UID or Name REQUIRED
Name	Object name. UID or Name REQUIRED
Layer (is required)	Layer that the rule belongs to identified by the name or UID.
Details Level	The level of detail for some of the fields in the response can vary from showing only the UID value of the object to a fully detailed representation of the object.

Outputs	Description
Message (message)	Operation status.

Checkpoint Management API/Add Access Layer method

Create new object.

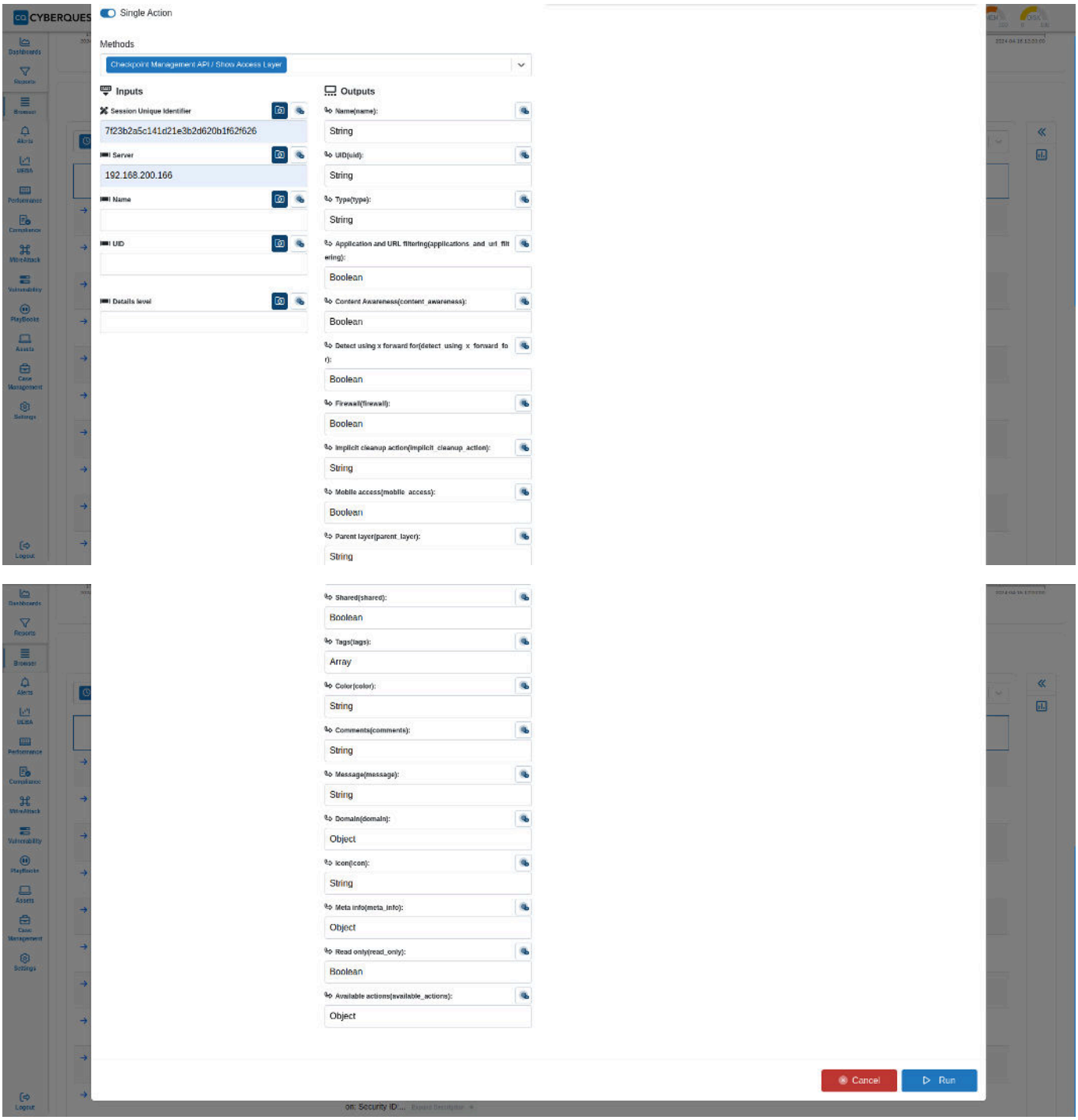


Inputs	Description
Session Unique Identifier (is required)	Session unique identifier as it returned by the login request
Server (is required)	Server Address
Name (is required)	Object name. Must be unique in the domain.
Add default rule	Indicates whether to include a cleanup rule in the new layer.
Applications and URL filtering	Whether to enable Applications & URL Filtering blade on the layer.
Content Awareness	Whether to enable Content Awareness blade on the layer.
Detect using x forward for	Whether to use X-Forward-For HTTP header, which is added by the proxy server to keep track of the original source IP.
Firewall	Whether to enable Firewall blade on the layer.
Implicit cleanup action	The default catch-all action for traffic that does not match any explicit or implied rules in the layer.
Mobile access	Whether to enable Mobile Access blade on the layer.
Shared	Whether this layer is shared.
Tags	Collection of tag identifiers.
Color	Color of the object. Should be one of existing colors.
Comments	Comments string.
Details level	The level of detail for some of the fields in the response can vary from showing only the UID value of the object to a fully detailed representation of the object.
Ignore warnings	Apply changes ignoring warnings.
Ignore errors	Apply changes ignoring errors. You wont be able to publish such a changes. If ignore-warnings flag was omitted - warnings will also be ignored.

Outputs	Description
Message (message)	Operation status.

Checkpoint Management API/Show Access Layer method

Retrieve existing object using object name or uid.

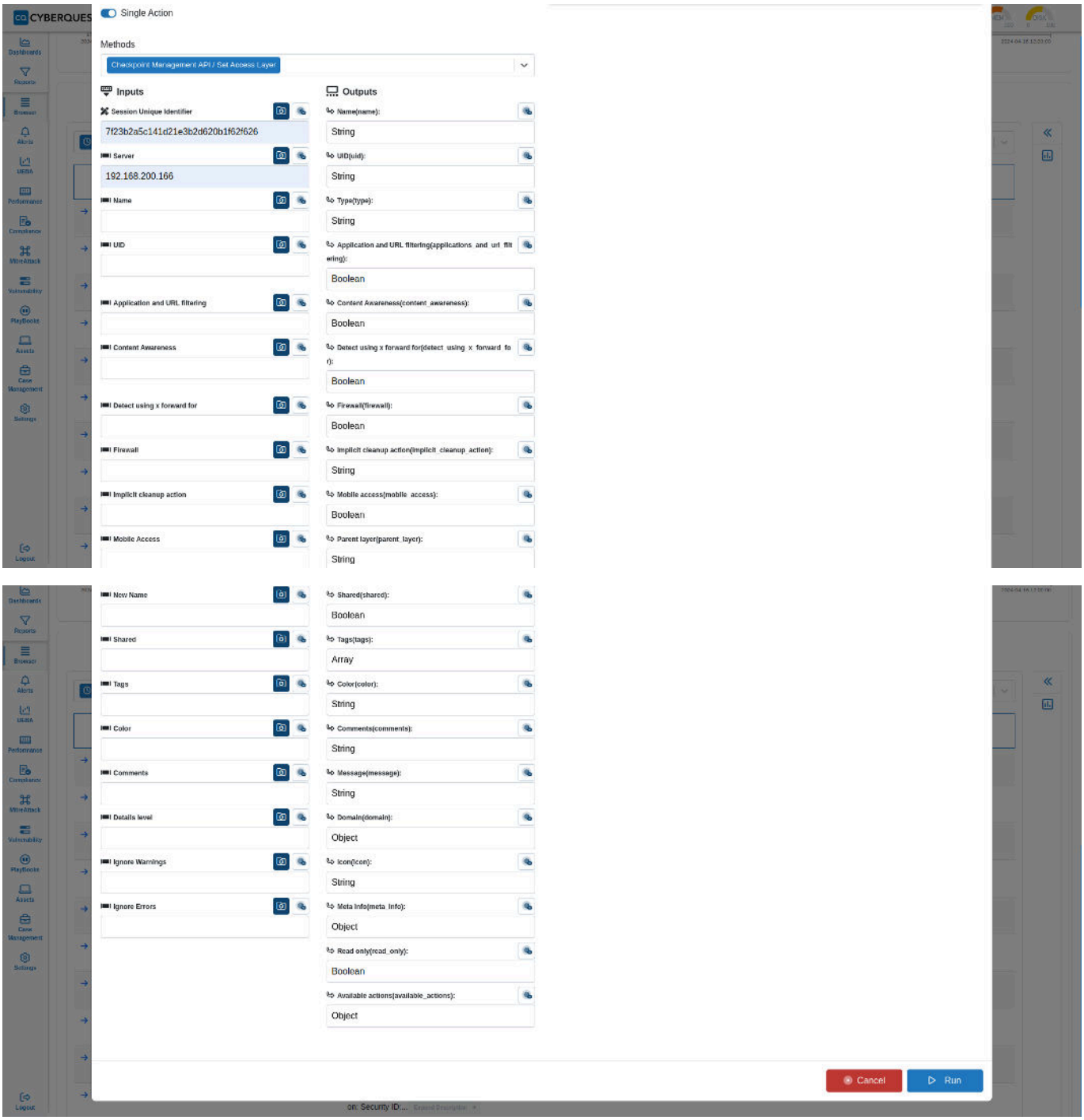


Inputs	Description
Session Unique Identifier (is required)	Session unique identifier as it returned by the login request
Server (is required)	Server Address
Name	Object name. Name or UID is REQUIRED!
UID	Object unique identifier. Name or UID is REQUIRED!
Details level	The level of detail for some of the fields in the response can vary from showing only the UID value of the object to a fully detailed representation of the object.

Outputs	Description
Name (name)	Object name. Must be unique in the domain.
UID (uid)	Object unique identifier.
Type (type)	Object type.
Application and URL filtering (applications_and_url_filtering)	Whether Applications & URL Filtering blade is enabled on this layer.
Content Awareness (content_awareness)	Whether Content Awareness blade is enabled on this layer.
Detect using x forward for (detect_using_x_forward_for)	Whether X-Forward-For HTTP header is been used.
Firewall (firewall)	Whether Firewall blade is enabled on this layer.
Implicit cleanup action (implicit_cleanup_action)	The default catch-all action for traffic that does not match any explicit or implied rules in the layer.
Mobile access (mobile_access)	Whether Mobile Access blade is enabled on this layer.
Parent layer (parent_layer)	Parent layer of this layer.
Shared (shared)	Whether this layer is shared.
Tags (tags)	Collection of tag objects identified by the name or UID. Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.
Color (color)	Color of the object. Should be one of existing colors.
Comments (comments)	Comments string.
Message (message)	Operation status.
Domain (domain)	Information about the domain that holds the Object.
Icon (icon)	Object icon.
Meta info (meta_info)	Object metadata.
Read only (read_only)	Indicates whether the object is read-only.
Available actions (available_actions)	Actions that are available on the object.

Checkpoint Management API/Set Access Layer method

Edit existing object using object name or uid.

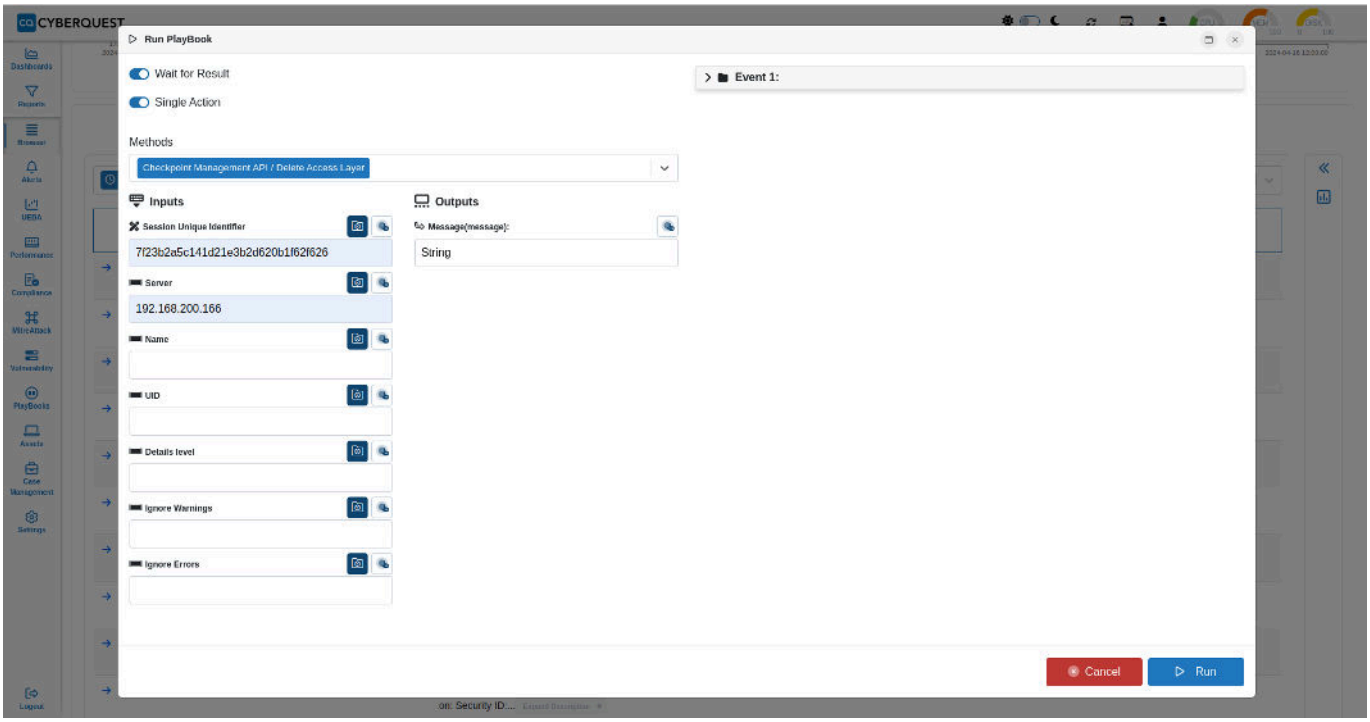

Single Action
Methods
Checkpoint Management API / Set Access Layer
Inputs
Outputs
Session Unique Identifier
7f23b2a5c141d21e3b2d620b1f62f626
Server
192.168.200.166
Name
UID
Application and URL filtering
Content Awareness
Detect using x forward for
Firewall
Implicit cleanup action
Mobile Access
New Name
Shared
Tags
Color
Comments
Details level
Ignore Warnings
Ignore Errors
Name(name):
String
UID(uid):
String
Type(type):
String
Application and URL filtering(applications_and_url_filtering):
Boolean
Content Awareness(content_awareness):
Boolean
Detect using x forward for(detect_using_x_forward_for):
Boolean
Firewall(firewall):
Boolean
Implicit cleanup action(implicit_cleanup_action):
String
Mobile access(mobile_access):
Boolean
Parent layer(parent_layer):
String
Shared(shared):
Boolean
Tags(tags):
Array
Color(color):
String
Comments(comments):
String
Message(message):
String
Domain(domain):
Object
Icon(icon):
String
Meta info(meta_info):
Object
Read only(read_only):
Boolean
Available actions(available_actions):
Object
Cancel
Run

Inputs	Description
Session Unique Identifier (is required)	Session unique identifier as it returned by the login request
Server (is required)	Server Address
Name	Object name. Name or UID is REQUIRED!
UID	Object unique identifier. Name or UID is REQUIRED!
Application and URL filtering	Whether to enable Applications & URL Filtering blade on the layer.
Content Awareness	Whether to enable Content Awareness blade on the layer.
Detect using x forward for	Whether to use X-Forward-For HTTP header, which is added by the proxy server to keep track of the original source IP.
Firewall	Whether to enable Firewall blade on the layer.
Implicit cleanup action	The default catch-all action for traffic that does not match any explicit or implied rules in the layer.
Mobile Access	Whether to enable Mobile Access blade on the layer.
New Name	New name of the object.
Shared	Whether this layer is shared.
Tags	Collection of tag identifiers.
Color	Color of the object. Should be one of existing colors.
Comments	The level of detail for some of the fields in the response can vary from showing only the UID value of the object to a fully detailed representation of the object.
Details level	The level of detail for some of the fields in the response can vary from showing only the UID value of the object to a fully detailed representation of the object.
Ignore Warnings	Apply changes ignoring warnings.
Ignore Errors	Apply changes ignoring errors. You wont be able to publish such a changes. If ignore-warnings flag was omitted - warnings will also be ignored.

Outputs	Description
Name (name)	Object name. Must be unique in the domain.
UID (uid)	Object unique identifier.
Type (type)	Object type.
Application and URL filtering (applications_and_url_filtering)	Whether Applications & URL Filtering blade is enabled on this layer.
Content Awareness (content_awareness)	Whether Content Awareness blade is enabled on this layer.
Detect using x forward for (detect_using_x_forward_for)	Whether X-Forward-For HTTP header is been used.
Firewall (firewall)	Whether Firewall blade is enabled on this layer.
Implicit cleanup action (implicit_cleanup_action)	The default catch-all action for traffic that does not match any explicit or implied rules in the layer.
Mobile access (mobile_access)	Whether Mobile Access blade is enabled on this layer.
Parent layer (parent_layer)	Parent layer of this layer.
Shared (shared)	Whether this layer is shared.
Tags (tags)	Collection of tag objects identified by the name or UID. Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.
Color (color)	Color of the object. Should be one of existing colors.
Comments (comments)	Comments string.
Message (message)	Operation status.
Domain (domain)	Information about the domain that holds the Object.
Icon (icon)	Object icon.
Meta info (meta_info)	Object metadata.
Read only (read_only)	Indicates whether the object is read-only.
Available actions (available_actions)	Actions that are available on the object.

Checkpoint Management API/Delete Access Layer method

Delete existing object using object name or uid.

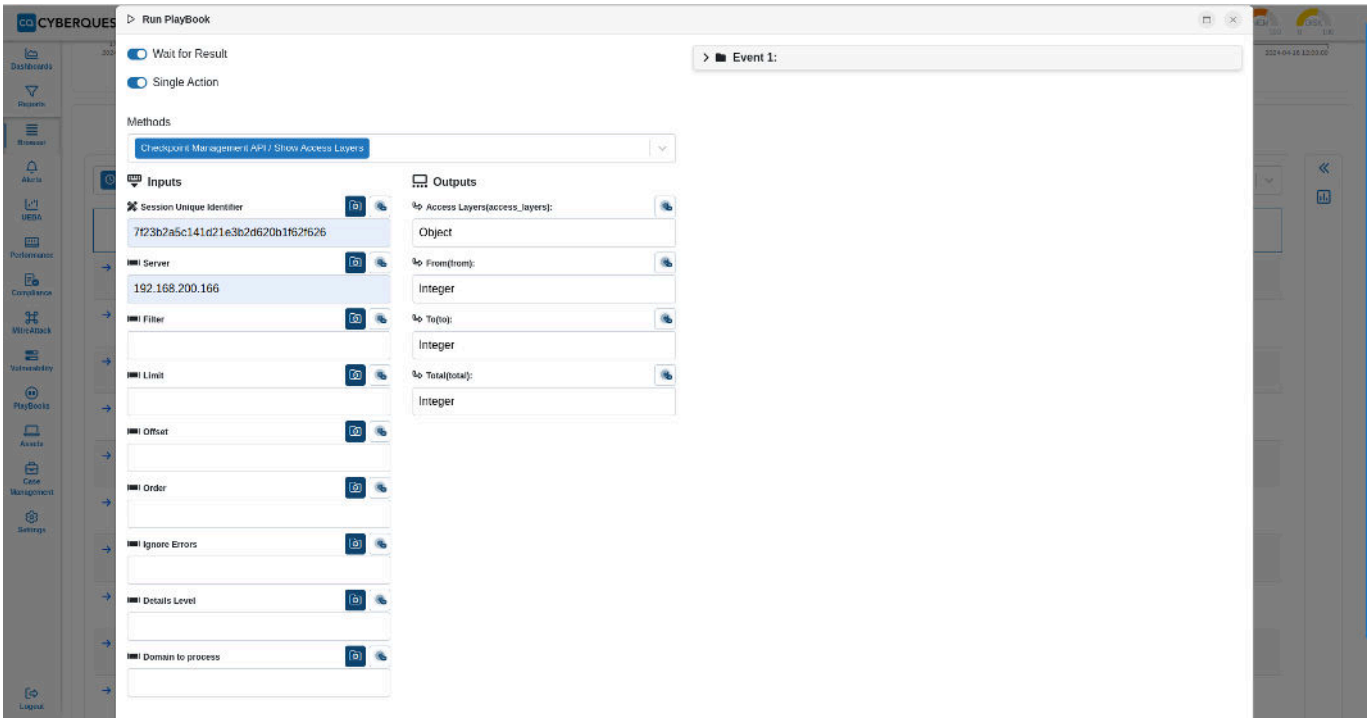


Inputs	Description
Session Unique Identifier (is required)	Session unique identifier as it returned by the login request
Server (is required)	Server Address
Name	Object name. Name or UID is REQUIRED!
UID	Object unique identifier. Name or UID is REQUIRED!
Details level	The level of detail for some of the fields in the response can vary from showing only the UID value of the object to a fully detailed representation of the object.
Ignore Warnings	Apply changes ignoring warnings.
Ignore Errors	Apply changes ignoring errors. You wont be able to publish such a changes. If ignore-warnings flag was omitted - warnings will also be ignored.

Outputs	Description
Message (message)	Operation status.

Checkpoint Management API/Show Access Layers method

Retrieve all objects.

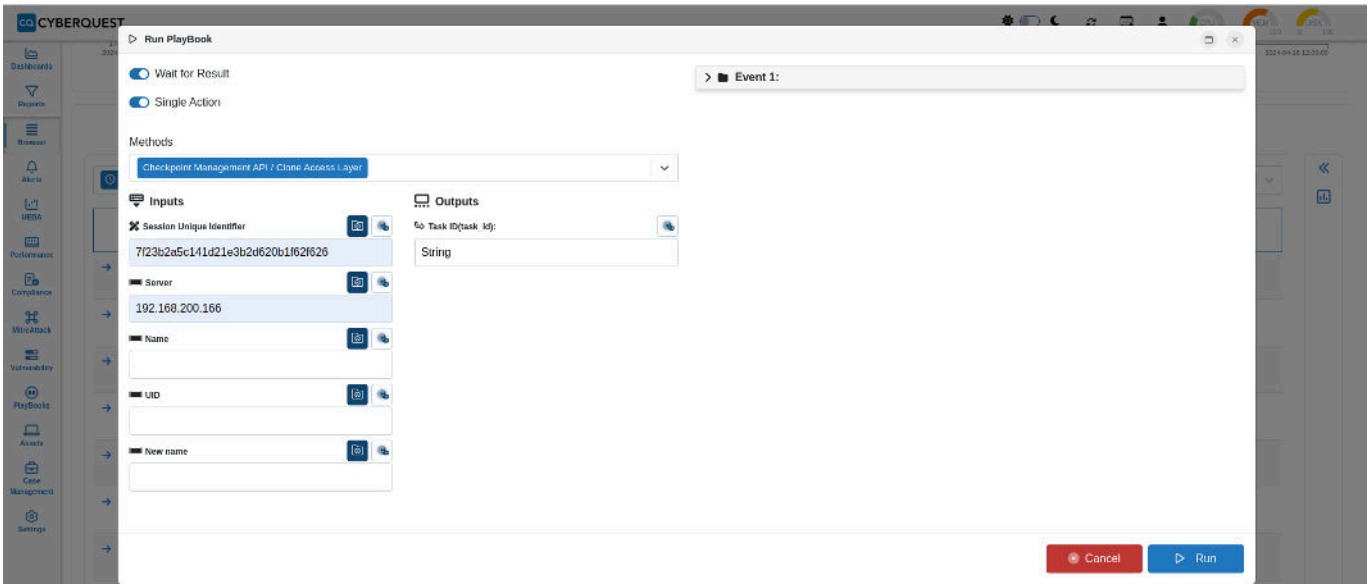


Inputs	Description
Session Unique Identifier (is required)	Session unique identifier as it returned by the login request
Server (is required)	Server Address
Filter	Search expression to filter objects by. The provided text should be exactly the same as it would be given in SmartConsole Object Explorer. The logical operators in the expression (AND, OR) should be provided in capital letters. The search involves both a IP search and a textual search in name, comment, tags etc.
Limit	The maximal number of returned results.
Offset	Number of the results to initially skip.
Order	Sorts the results by search criteria. Automatically sorts the results by Name, in the ascending order.
Ignore Errors	Apply changes ignoring errors. You wont be able to publish such a changes. If ignore-warnings flag was omitted - warnings will also be ignored.
Details Level	The level of detail for some of the fields in the response can vary from showing only the UID value of the object to a fully detailed representation of the object.
Domain to process	Indicates which domains to process the commands on. It cannot be used with the details-level full, must be run from the System Domain only and with ignore-warnings true. Valid values are: CURRENT_DOMAIN, ALL_DOMAINS_ON_THIS_SERVER.

Outputs	Description
Access Layers (access_layers)	Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.
From (from)	From which element number the query was done.
To (to)	Operation status.
Total (total)	Total number of elements returned by the query.

Checkpoint Management API/Clone Access Layer method

Clone access layer using layer name or uid.

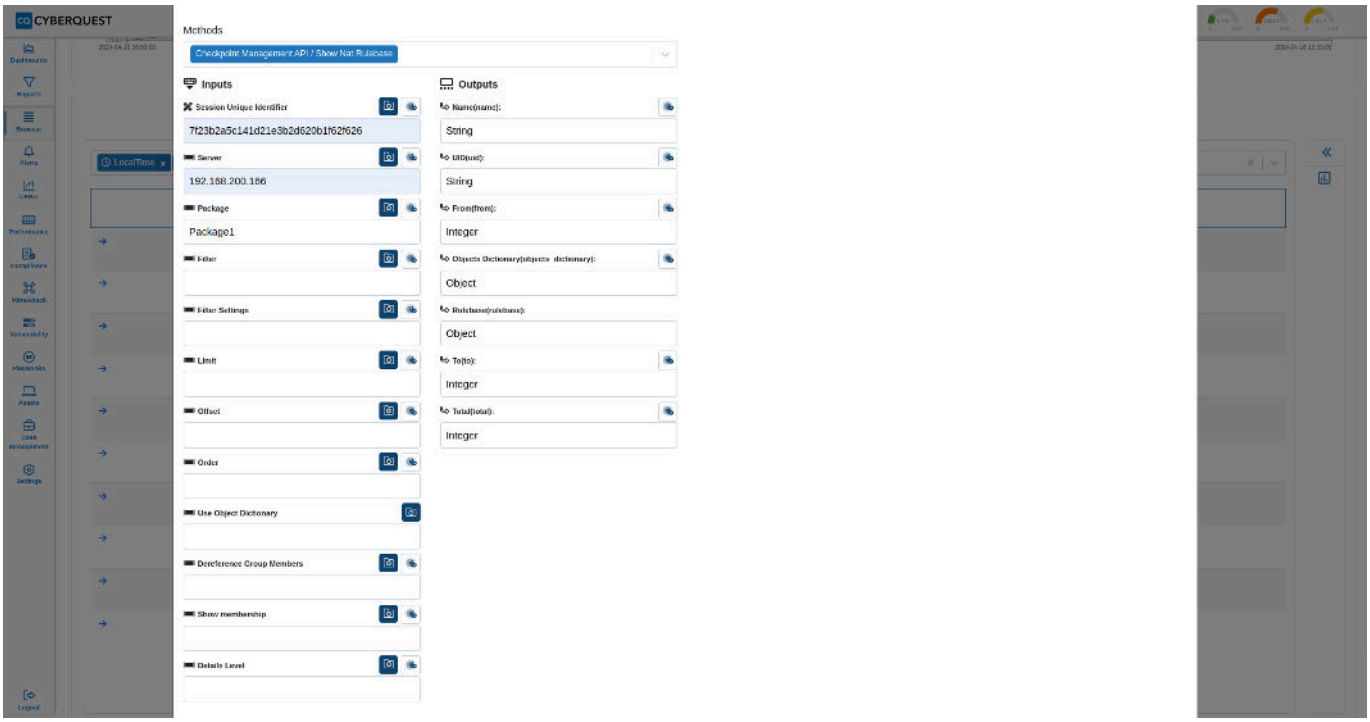


Inputs	Description
Session Unique Identifier (is required)	Session unique identifier as it returned by the login request
Server (is required)	Server Address
Name	The name of the layer to be cloned.
UID	The uid of the layer to be cloned.
New name	The name of the cloned layer.

Outputs	Description
Task ID (task_id)	Asynchronous task unique identifier. Use show-task command to check the progress of the task.

Checkpoint Management API/Show Nat Rulebase method

Shows the entire NAT Rules layer. This layer is divided into sections. A NAT Rule may be within a section, or independent of a section (in which case it is said to be under the global section). There are two types of sections: auto generated read only sections and general sections which are created manually. The reply features a list of objects. Each object may be a section of the layer, within which its rules may be found, or a rule itself, for the case of rules which are under the global section. An optional filter field may be added in order to filter out only those rules that match a search criteria.

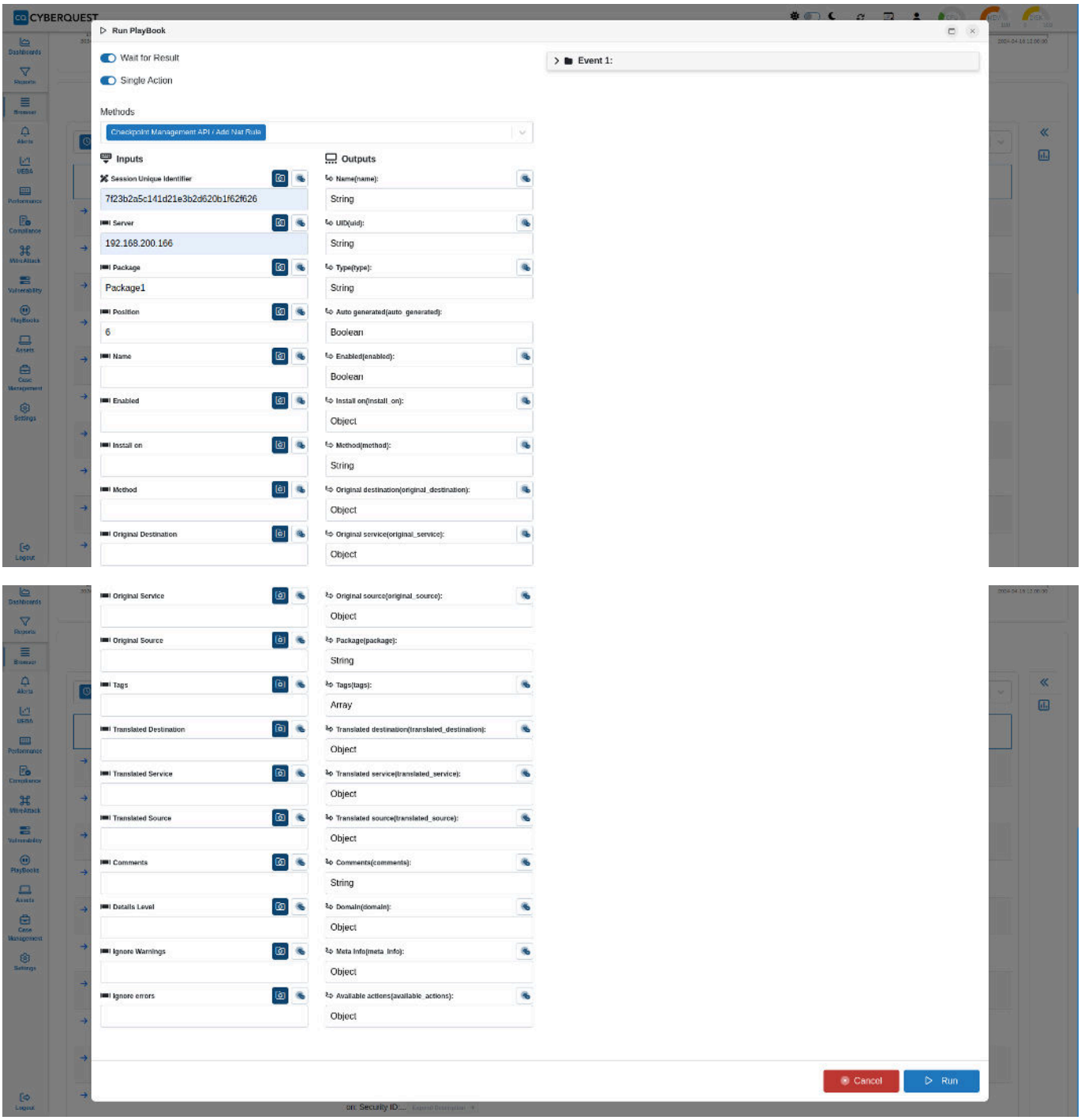


Inputs	Description
Session Unique Identifier (is required)	Session unique identifier as it returned by the login request
Server (is required)	Server Address
Package (is required)	Name of the package
Filter	Search expression to filter the rulebase. The provided text should be exactly the same as it would be given in Smart Console. The logical operators in the expression (AND, OR) should be provided in capital letters. If an operator is not used, the default OR operator applies.
Filter Settings	Sets filter preferences.
Limit	The maximal number of returned results.
Offset	Number of the results to initially skip.
Order	Sorts the results by search criteria. Automatically sorts the results by Name, in the ascending order.
Use Object Dictionary	
Dereference Group Members	Indicates whether to dereference members field by details level for every object in reply.
Show membership	Indicates whether to calculate and show groups field for every object in reply.
Details Level	The level of detail for some of the fields in the response can vary from showing only the UID value of the object to a fully detailed representation of the object.

Outputs	Description
Name (name)	Object name. Must be unique in the domain.
UID (uid)	Object unique identifier.
From (from)	From which element number the query was done.
Objects Dictionary (objects_dictionary)	Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.
Rulebase (rulebase)	
To (to)	To which element number the query was done.
Total (total)	Total number of elements returned by the query

Checkpoint Management API/Add Nat Rule method

Create new object.

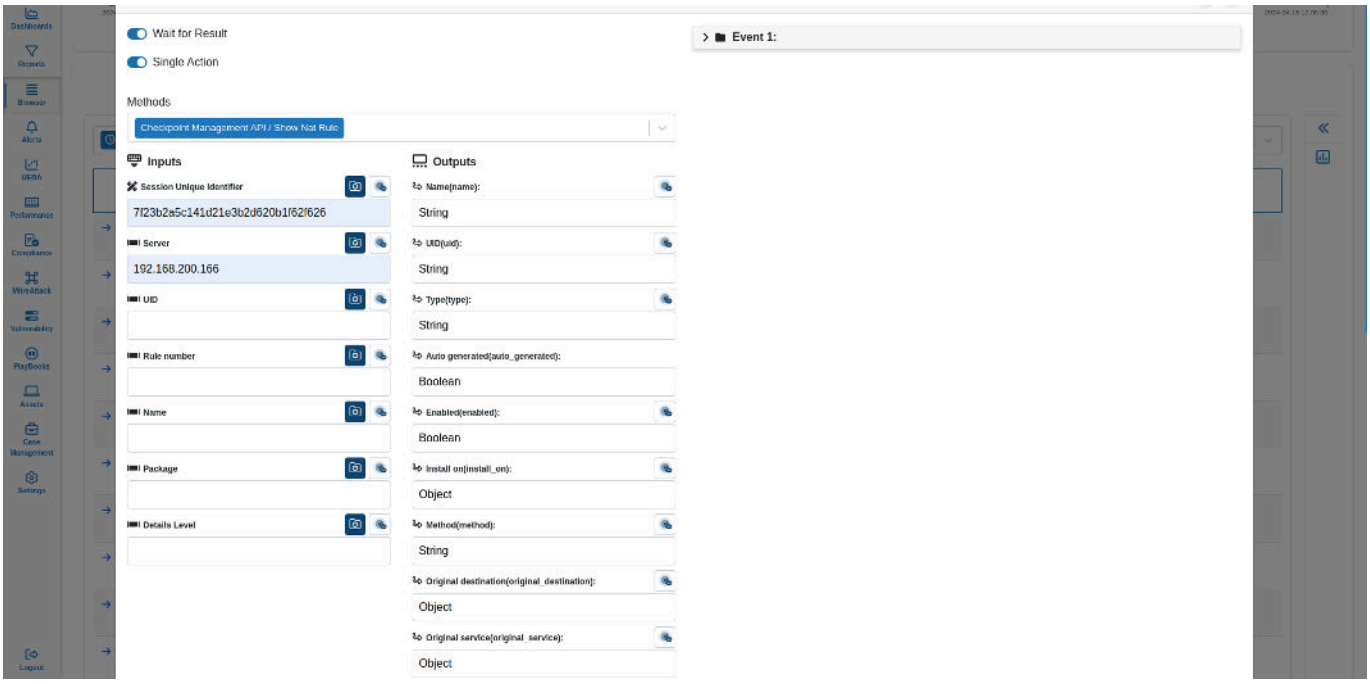


Inputs	Description
Session Unique Identifier (is required)	Session unique identifier as it returned by the login request
Server (is required)	Server Address
Package (is required)	Name of the package.
Position (is required)	Position in the rulebase.
Name	Rule name.
Enabled	Enable/Disable the rule.
Install on	Which Gateways identified by the name or UID to install the policy on.
Method	Nat method.
Original Destination	Original destination.
Original Service	Original service.
Original Source	Original source.
Tags	Collection of tag objects identified by the name or UID.
Translated Destination	Translated destination.
Translated Service	Translated service.
Translated Source	Translated source.
Comments	Comments string.
Details Level	The level of detail for some of the fields in the response can vary from showing only the UID value of the object to a fully detailed representation of the object.
Ignore Warnings	Apply changes ignoring warnings.
Ignore errors	Apply changes ignoring errors. You wont be able to publish such a changes. If ignore-warnings flag was omitted - warnings will also be ignored.

Outputs	Description
Name (name)	Object name. Must be unique in the domain.
UID (uid)	Object unique identifier.
Type (type)	Object type.
Auto generated (auto_generated)	
Enabled (enabled)	Enable/Disable the rule.
Install on (install_on)	Which gateway, identified by the name or UID, to install the policy. Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.
Method (method)	Nat method.
Original destination (original_destination)	Original destination. Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.
Original service (original_service)	Original service. Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.
Original source (original_source)	Original source. Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.
Package (package)	
Tags (tags)	Collection of tag objects identified by the name or UID.
Translated destination (translated_destination)	Translated destination. Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.
Translated service (translated_service)	Translated service. Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.
Translated source (translated_source)	Translated source. Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.
Comments (comments)	Comments string.
Domain (domain)	Information about the domain that holds the Object.
Meta info (meta_info)	Object metadata.
Available actions (available_actions)	Actions that are available on the object.

Checkpoint Management API/Show Nat Rule method

Retrieve existing object using object name or uid.

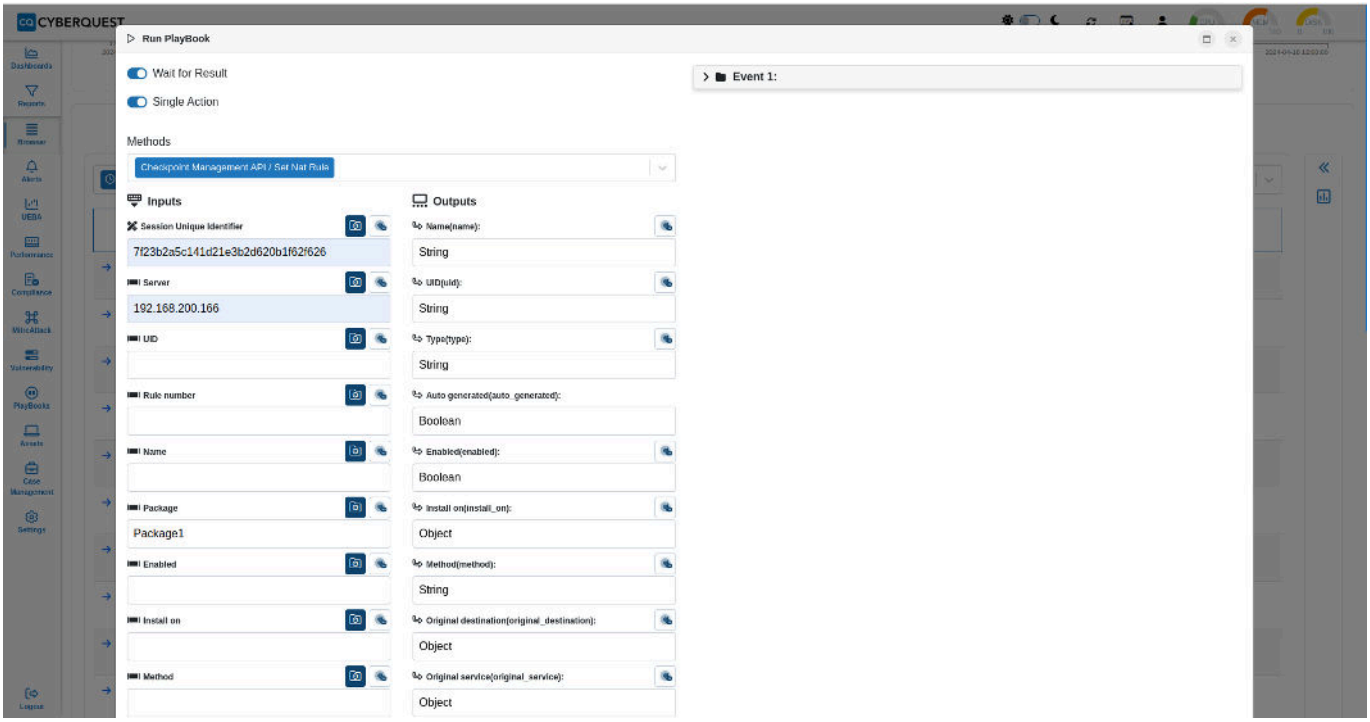


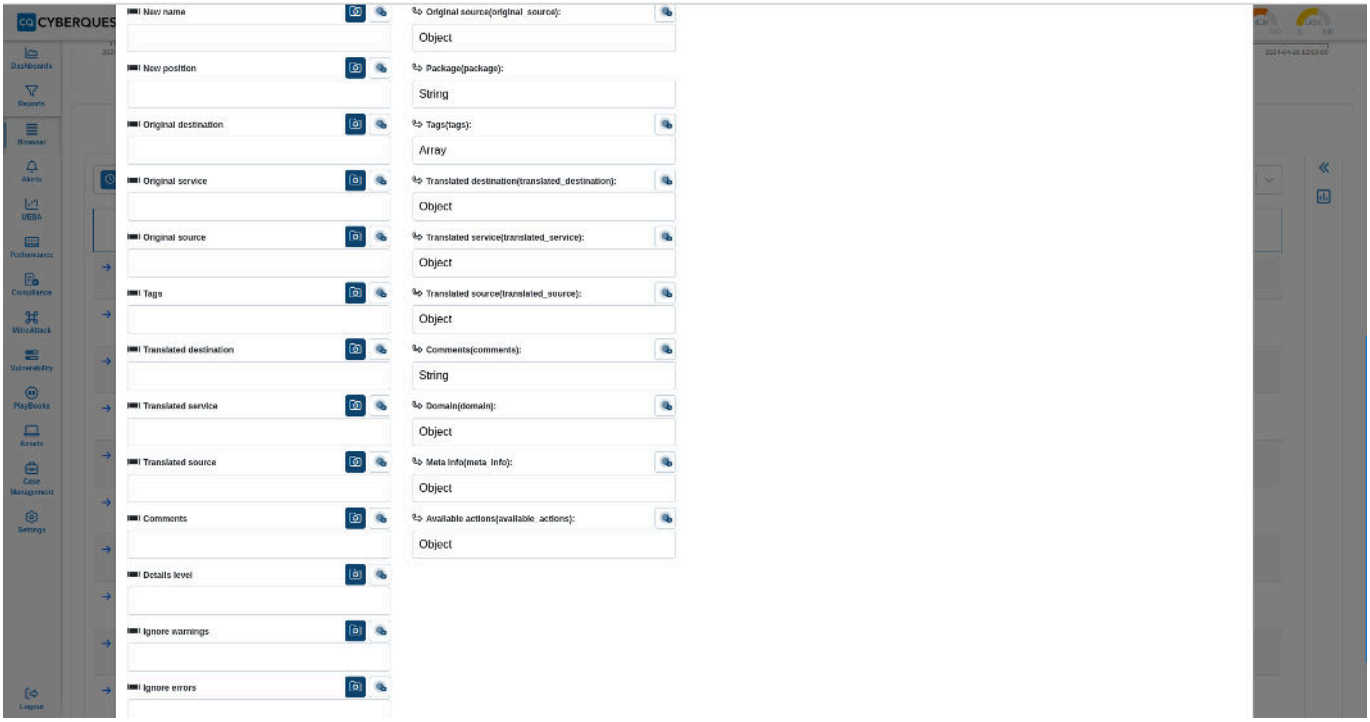
Inputs	Description
Session Unique Identifier (is required)	Session unique identifier as it returned by the login request
Server (is required)	Server Address
UID	Object unique identifier. UID or Rule number or Name is REQUIRED!
Rule number	Rule number. UID or Rule number or Name is REQUIRED!
Name	Rule name. UID or Rule number or Name is REQUIRED!
Package (is required)	Name of the package.
Details Level	The level of detail for some of the fields in the response can vary from showing only the UID value of the object to a fully detailed representation of the object.

Outputs	Description
Name (name)	Object name. Must be unique in the domain.
UID (uid)	Object unique identifier.
Type (type)	Object type.
Auto generated (auto_generated)	
Enabled (enabled)	Enable/Disable the rule.
Install on (install_on)	Which gateway, identified by the name or UID, to install the policy. Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.
Method (method)	Nat method.
Original destination (original_destination)	Original destination. Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.
Original service (original_service)	Original service. Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.
Original source (original_source)	Original source. Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.
Package (package)	
Tags (tags)	Collection of tag objects identified by the name or UID.
Translated destination (translated_destination)	Translated destination. Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.
Translated service (translated_service)	Translated service. Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.
Translated source (translated_source)	Translated source. Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.
Comments (comments)	Comments string.
Domain (domain)	Information about the domain that holds the Object.
Meta info (meta_info)	Object metadata.
Available actions (available_actions)	Actions that are available on the object.

Checkpoint Management API/Set Nat Rule method

Edit existing object using object name or uid.


CYBERQUEST
Run PlayBook
Wait for Result
Single Action
Methods
Checkpoint Management API / Set Nat Rule
Inputs
Session Unique Identifier
7f23b2a5c141d21e3b2d620b1f62f626
Server
192.168.200.166
UID
Rule number
Name
Package
Package1
Enabled
Install on
Method
Outputs
Name(name):
String
UID(uid):
String
Type(type):
String
Auto generated(auto_generated):
Boolean
Enabled(enabled):
Boolean
Install on(install_on):
Object
Method(method):
String
Original destination(original_destination):
Object
Original service(original_service):
Object
Event 1:


New name
New position
Original destination
Original service
Original source
Tags
Translated destination
Translated service
Translated source
Comments
Details level
Ignore warnings
Ignore errors
Original source(original_source):
Object
Package(package):
String
Tags(tags):
Array
Translated destination(translated_destination):
Object
Translated service(translated_service):
Object
Translated source(translated_source):
Object
Comments(comments):
String
Domain(domain):
Object
Meta info(meta_info):
Object
Available actions(available_actions):
Object

Inputs	Description
Session Unique Identifier (is required)	Session unique identifier as it returned by the login request
Server (is required)	Server Address
UID	Object unique identifier. UID or Rule number or Name is REQUIRED!
Rule number	Rule number. UID or Rule number or Name is REQUIRED!
Name	Rule name. UID or Rule number or Name is REQUIRED!
Package (is required)	Name of the package.
Enabled	Enable/Disable the rule.
Install on	Which Gateways identified by the name or UID to install the policy on.
Method	Nat method.
New name	New name of the object.
New position	New position in the rulebase.
Original destination	Original destination.
Original service	Original service.
Original source	The level of detail for some of the fields in the response can vary from showing only the UID value of the object to a fully detailed representation of the object.
Tags	The level of detail for some of the fields in the response can vary from showing only the UID value of the object to a fully detailed representation of the object.
Translated destination	The level of detail for some of the fields in the response can vary from showing only the UID value of the object to a fully detailed representation of the object.
Translated service	The level of detail for some of the fields in the response can vary from showing only the UID value of the object to a fully detailed representation of the object.
Translated source	The level of detail for some of the fields in the response can vary from showing only the UID value of the object to a fully detailed representation of the object.
Comments	The level of detail for some of the fields in the response can vary from showing only the UID value of the object to a fully detailed representation of the object.
Details level	The level of detail for some of the fields in the response can vary from showing only the UID value of the object to a fully detailed representation of the object.
Ignore warnings	The level of detail for some of the fields in the response can vary from showing only the UID value of the object to a fully detailed representation of the object.
Ignore errors	The level of detail for some of the fields in the response can vary from showing only the UID value of the object to a fully detailed representation of the object.

Outputs	Description
Name (name)	Object name. Must be unique in the domain.
UID (uid)	Object unique identifier.
Type (type)	Object type.
Auto generated (auto_generated)	
Enabled (enabled)	Enable/Disable the rule.
Install on (install_on)	Which gateway, identified by the name or UID, to install the policy. Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.
Method (method)	Nat method.
Original destination (original_destination)	Original destination. Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.
Original service (original_service)	Original service. Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.
Original source (original_source)	Original source. Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.
Package (package)	
Tags (tags)	Collection of tag objects identified by the name or UID.
Translated destination (translated_destination)	Translated destination. Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.
Translated service (translated_service)	Translated service. Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.
Translated source (translated_source)	Translated source. Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.
Comments (comments)	Comments string.
Domain (domain)	Information about the domain that holds the Object.
Meta info (meta_info)	Object metadata.
Available actions (available_actions)	Actions that are available on the object.

Checkpoint Management API/Add Nat Section method

Create new object.

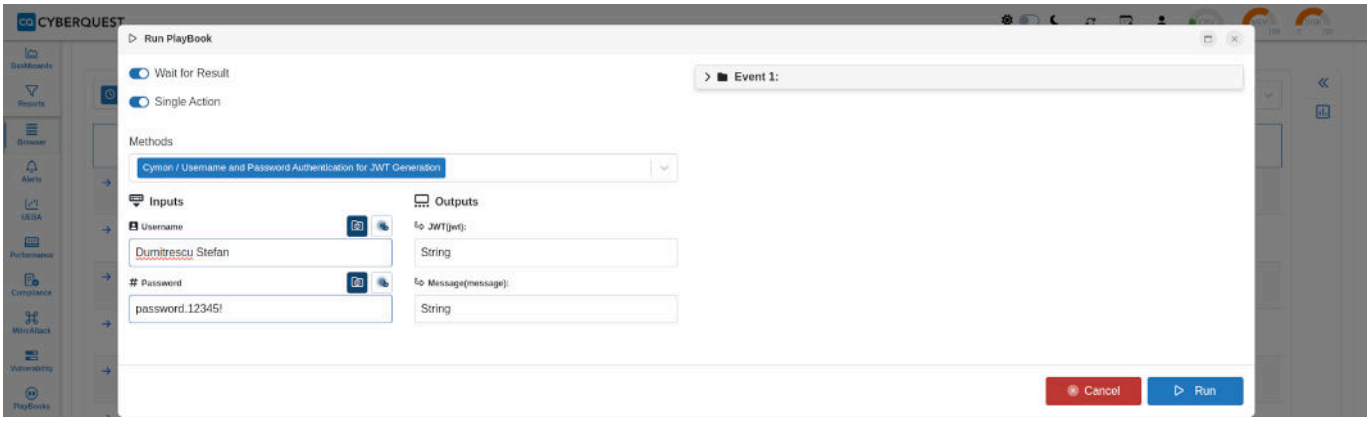
Inputs	Description
Session Unique Identifier (is required)	Session unique identifier as it returned by the login request
Server (is required)	Server Address
Package (is required)	Name of the package.
Position (is required)	Position in the rulebase.
Name	Object name. Must be unique in the domain.
Tags	Collection of tag objects identified by the name or UID.
Details level	The level of detail for some of the fields in the response can vary from showing only the UID value of the object to a fully detailed representation of the object.
Ignore Warnings	Apply changes ignoring warnings.
Ignore errors	Apply changes ignoring errors. You wont be able to publish such a changes. If ignore-warnings flag was omitted - warnings will also be ignored.

Outputs	Description
Name (name)	Object name. Must be unique in the domain.
UID (uid)	Object unique identifier.
Type (type)	Object type.
Tags (tags)	Collection of tag objects identified by the name or UID. Level of details in the output corresponds to the number of details for search. This table shows the level of details in the Standard level.
Domain (domain)	Information about the domain that holds the Object.
Meta info (meta_info)	Object metadata.
Read only (read_only)	Indicates whether the object is read-only.
Available actions (available_actions)	Actions that are available on the object.

Cymon

Cymon/Username and Password Authentication for JWT Generation method

Authenticate with username and password to get a JSON Web Token.

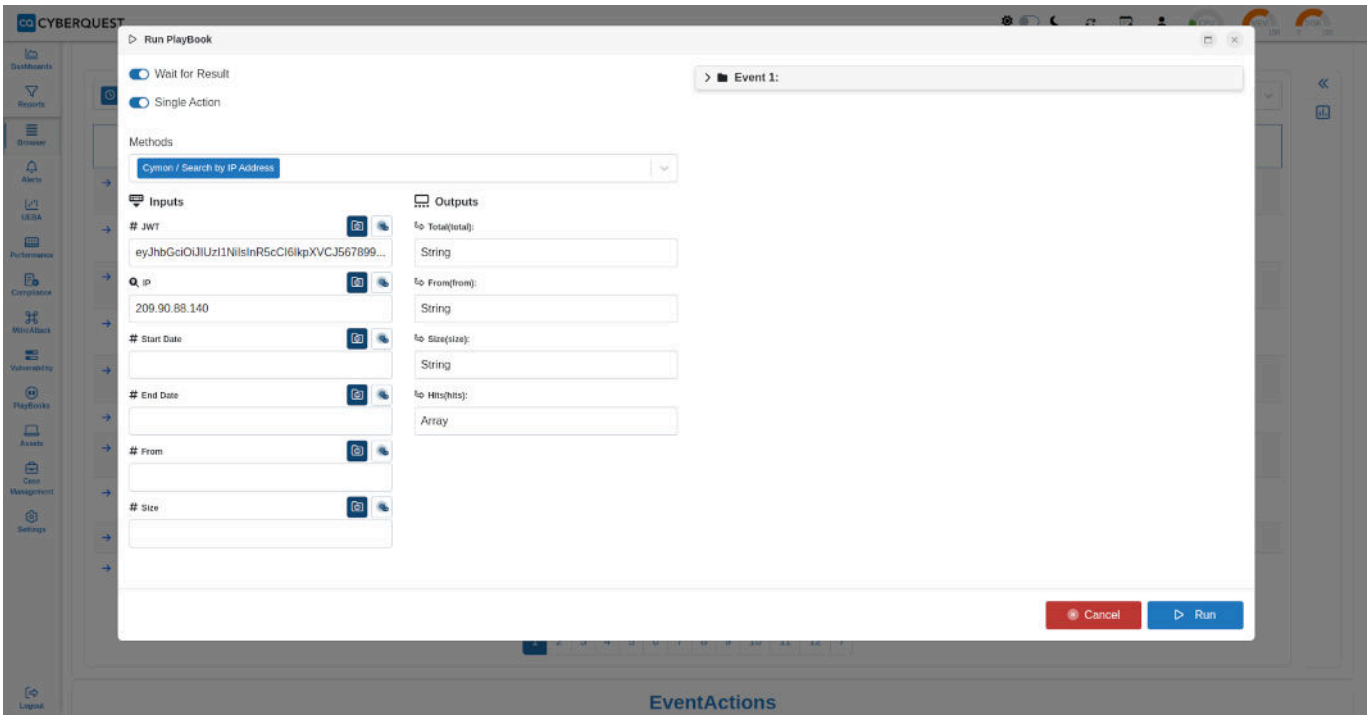


Inputs	Description
Username (is required)	The Username which is used to create JSON Web Token
Password (is required)	The Password which is used to create JSON Web Token

Outputs	Description
JWT(jwt)	JSON Web Token
Message(message)	Success message

Cymon/Search by IP Address method

Search threat reports by IP address (IPv4 and IPv6).

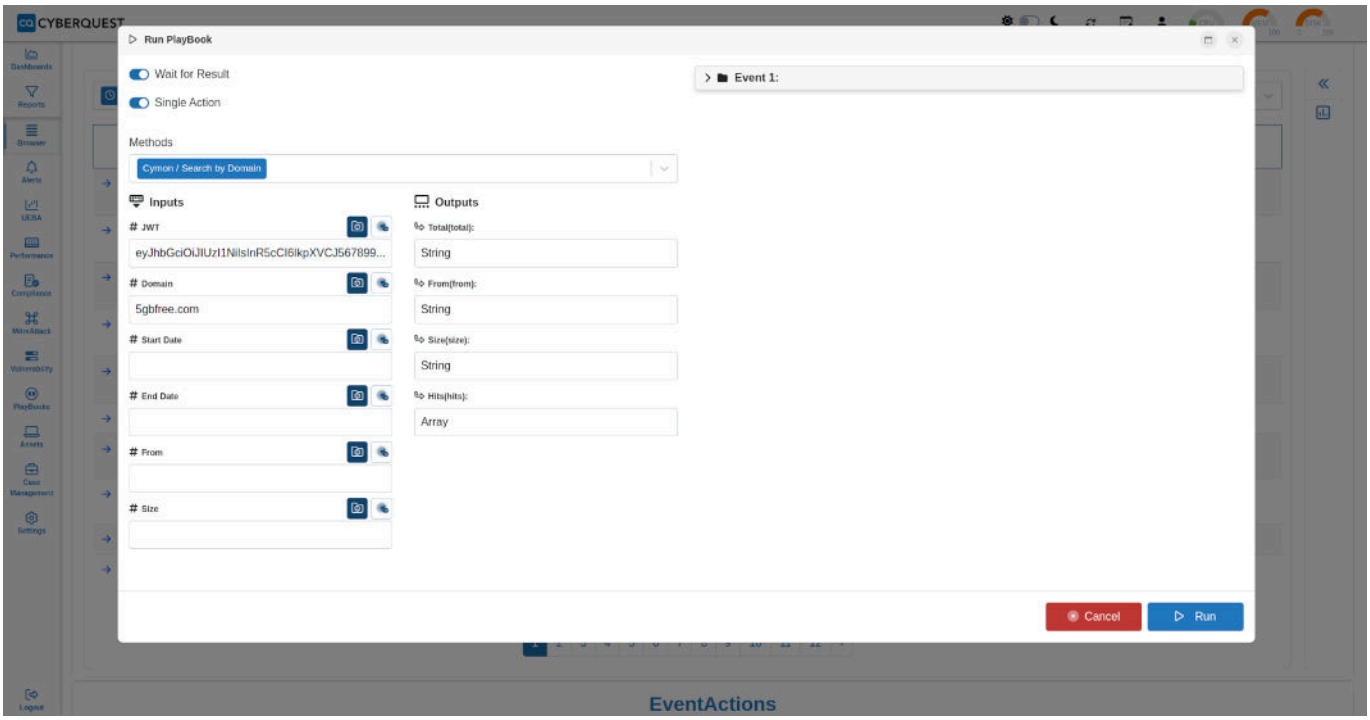


Inputs	Description
JWT (is required)	The JSON Web Token which was created previously (in Login)
IP (is required)	The query value (IP) to search for
Start Date	The start date for searching
End Date	The end date for searching
From	The offset to use for pagination
Size	The limit to use for pagination

Outputs	Description
Total(total)	Total number of objects in database for query
From(from)	The query offset value
Size(size)	The query limit value for how many objects to return
Hits(hits)	The threat reports searched by IP address

Cymon/Search by Domain method

Search threat reports by domain name.

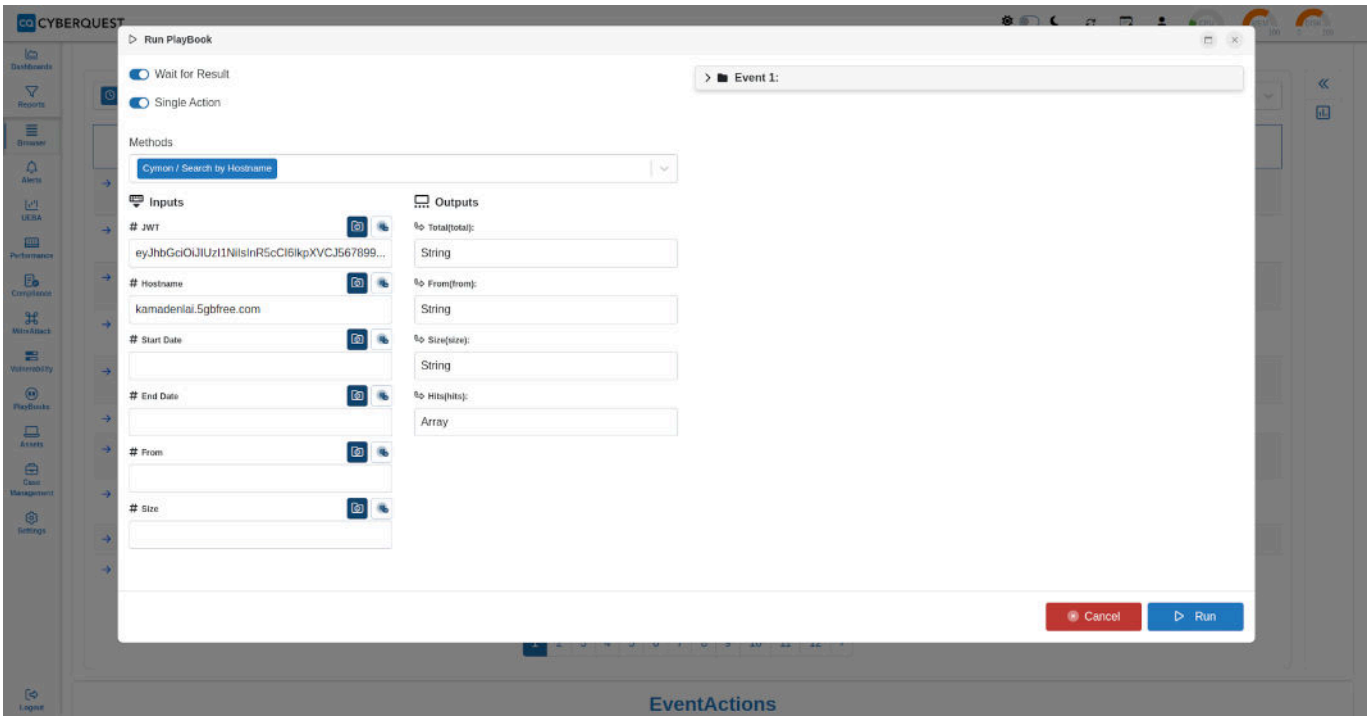


Inputs	Description
JWT (is required)	The JSON Web Token which was created previously (in Login)
Domain (is required)	The query value (domain) to search for
Start Date	The start date for searching
End Date	The end date for searching
From	The offset to use for pagination
Size	The limit to use for pagination

Outputs	Description
Total (total)	Total number of objects in database for query
From (from)	The query offset value
Size (size)	The query limit value for how many objects to return
Hits (hits)	The threat reports searched by IP address

Cymon/Search by Hostname method

Search threat reports by hostname.

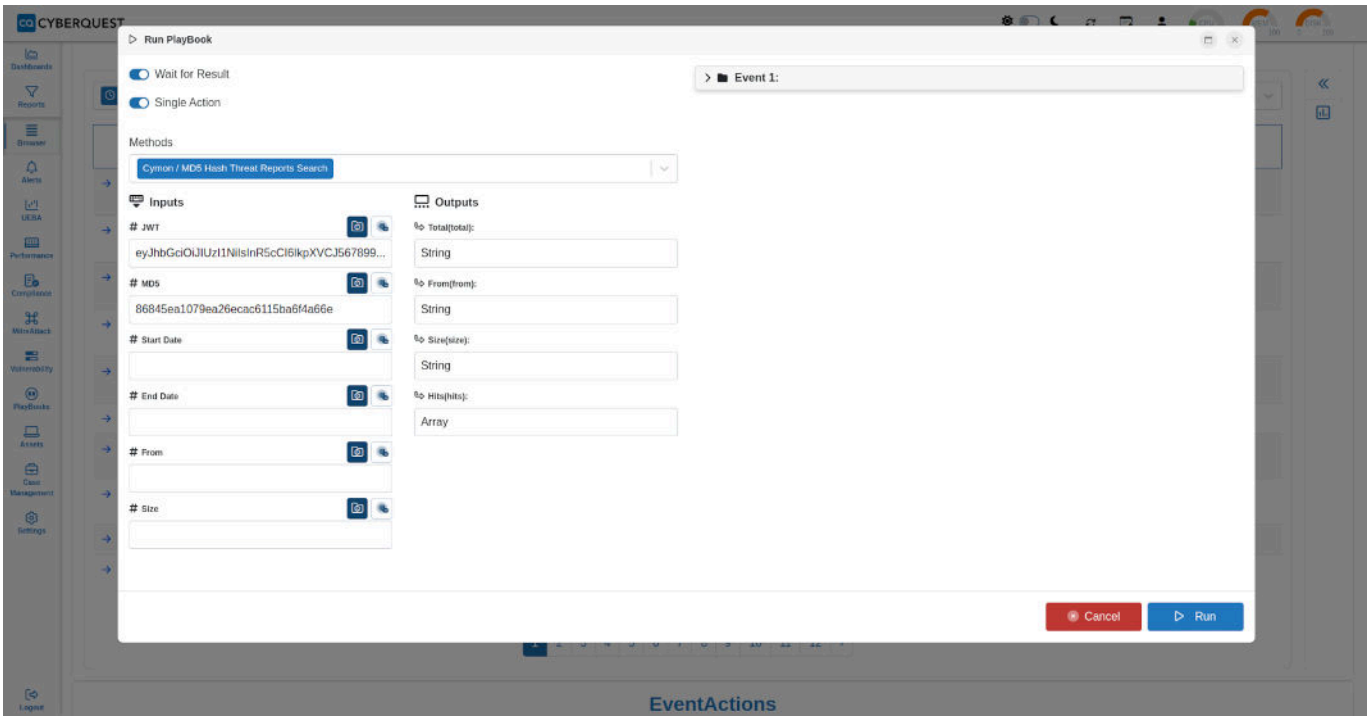


Inputs	Description
JWT (is required)	The JSON Web Token which was created previously (in Login)
Hostname (is required)	The query value (hostname) to search for
Start Date	The start date for searching
End Date	The end date for searching
From	The offset to use for pagination
Size	The limit to use for pagination

Outputs	Description
Total (total)	Total number of objects in database for query
From (from)	The query offset value
Size (size)	The query limit value for how many objects to return
Hits (hits)	The threat reports searched by IP address

Cymon/MD5 Hash Threat Reports Search method

Search threat reports by MD5 hash.

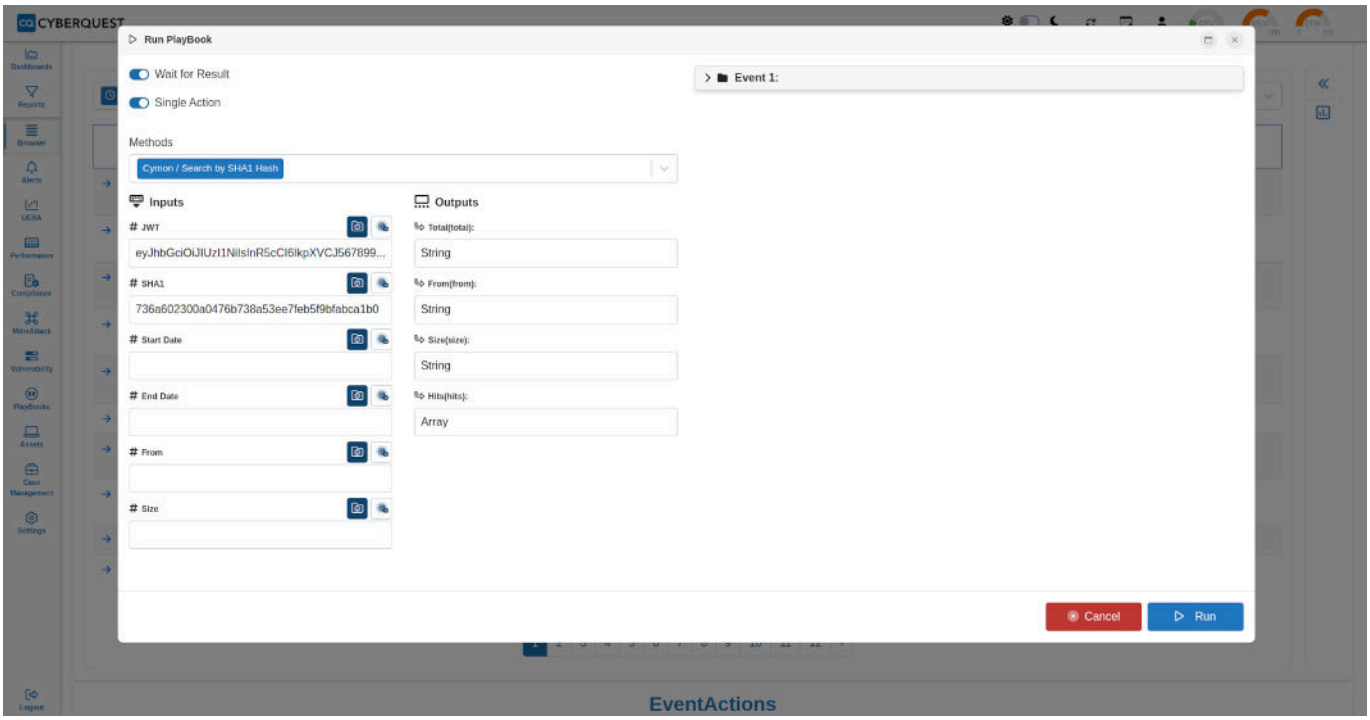


Inputs	Description
JWT (is required)	The JSON Web Token which was created previously (in Login)
MD5 (is required)	The query value (MD5) to search for
Start Date	The start date for searching
End Date	The end date for searching
From	The offset to use for pagination
Size	The limit to use for pagination

Outputs	Description
Total (total)	Total number of objects in database for query
From (from)	The query offset value
Size (size)	The query limit value for how many objects to return
Hits (hits)	The threat reports searched by IP address

Cymon/Search by SHA1 Hash method

Search threat reports by SHA1 hash.

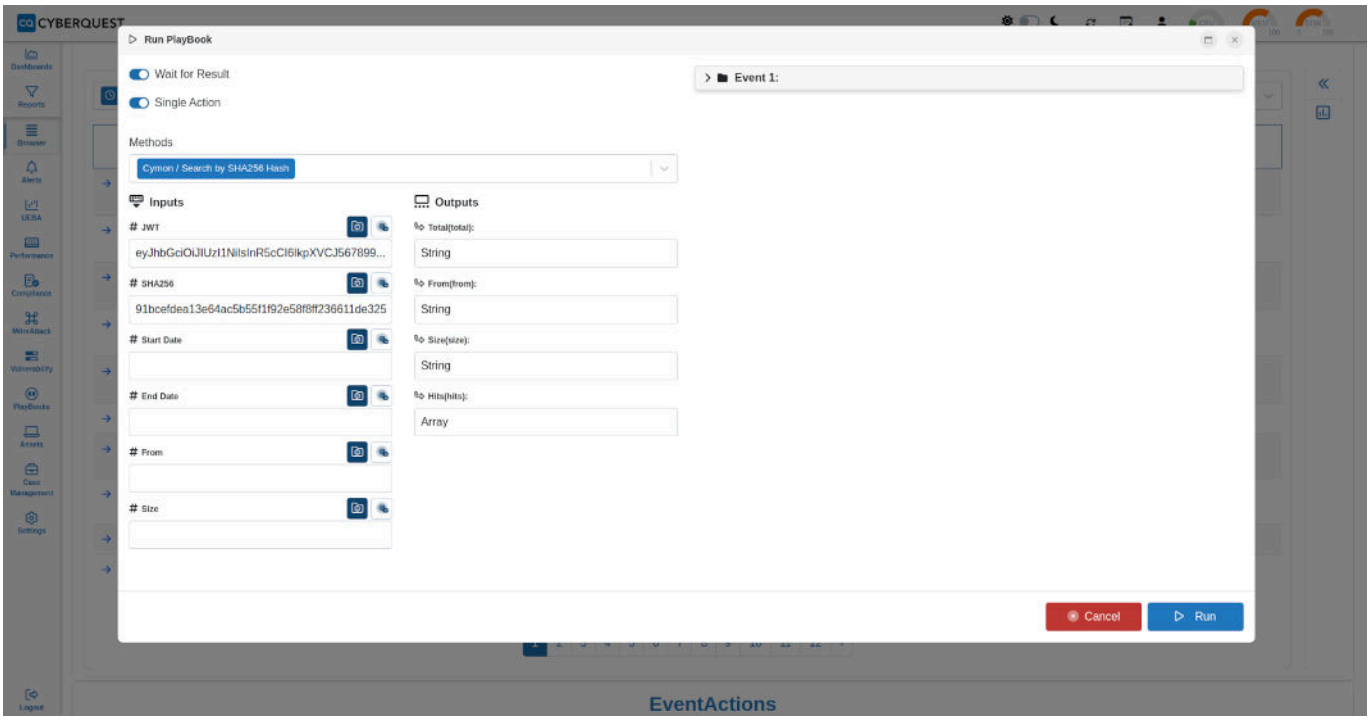


Inputs	Description
JWT (is required)	The JSON Web Token which was created previously (in Login)
SHA1 (is required)	The query value (sha1) to search for
Start Date	The start date for searching
End Date	The end date for searching
From	The offset to use for pagination
Size	The limit to use for pagination

Outputs	Description
Total (total)	Total number of objects in database for query
From (from)	The query offset value
Size (size)	The query limit value for how many objects to return
Hits (hits)	The threat reports searched by IP address

Cymon/Search by SHA256 Hash method

Search threat reports by SHA256 hash.

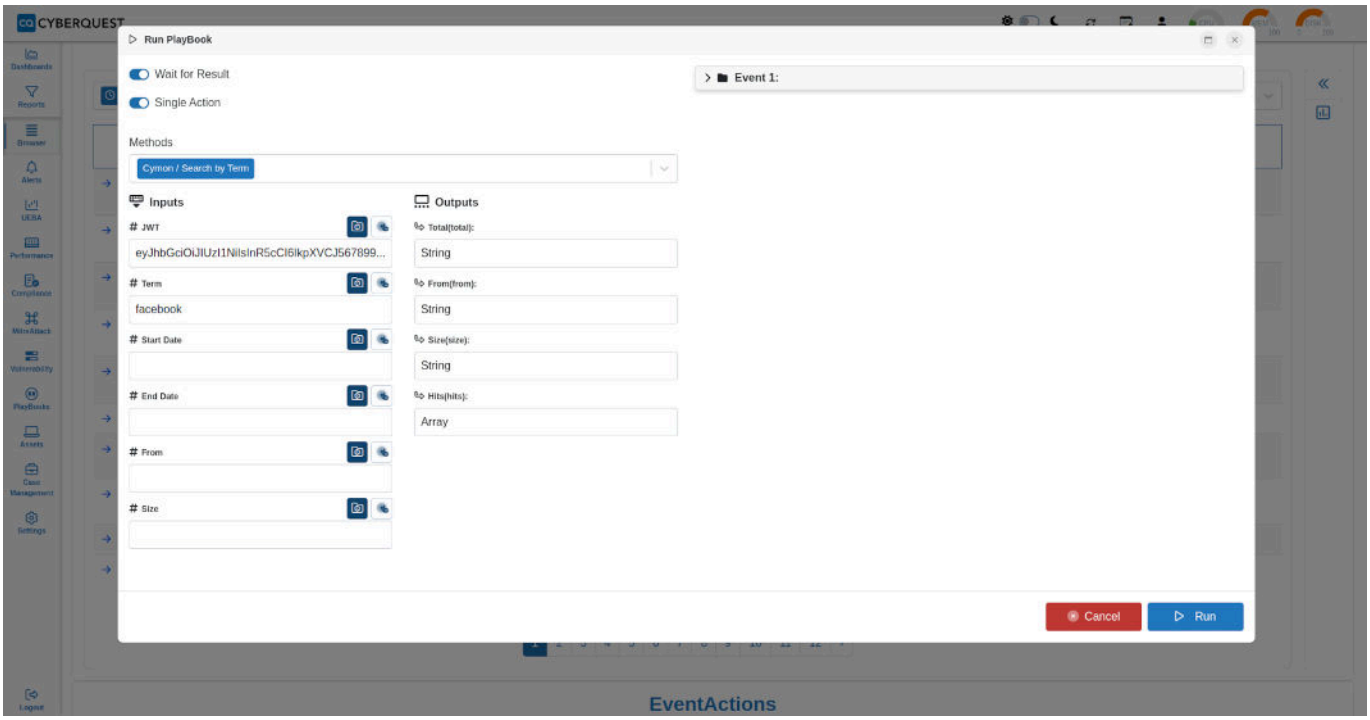


Inputs	Description
JWT (is required)	The JSON Web Token which was created previously (in Login)
SHA256 (is required)	The query value(SHA256) to search for
Start Date	The start date for searching
End Date	The end date for searching
From	The offset to use for pagination
Size	The limit to use for pagination

Outputs	Description
From (from)	The query offset value
Total (total)	Total number of objects in database for query
Size (size)	The query limit value for how many objects to return
Hits (hits)	The threat reports searched by IP address

Cymon/Search by Term method

Search threat reports by a term.

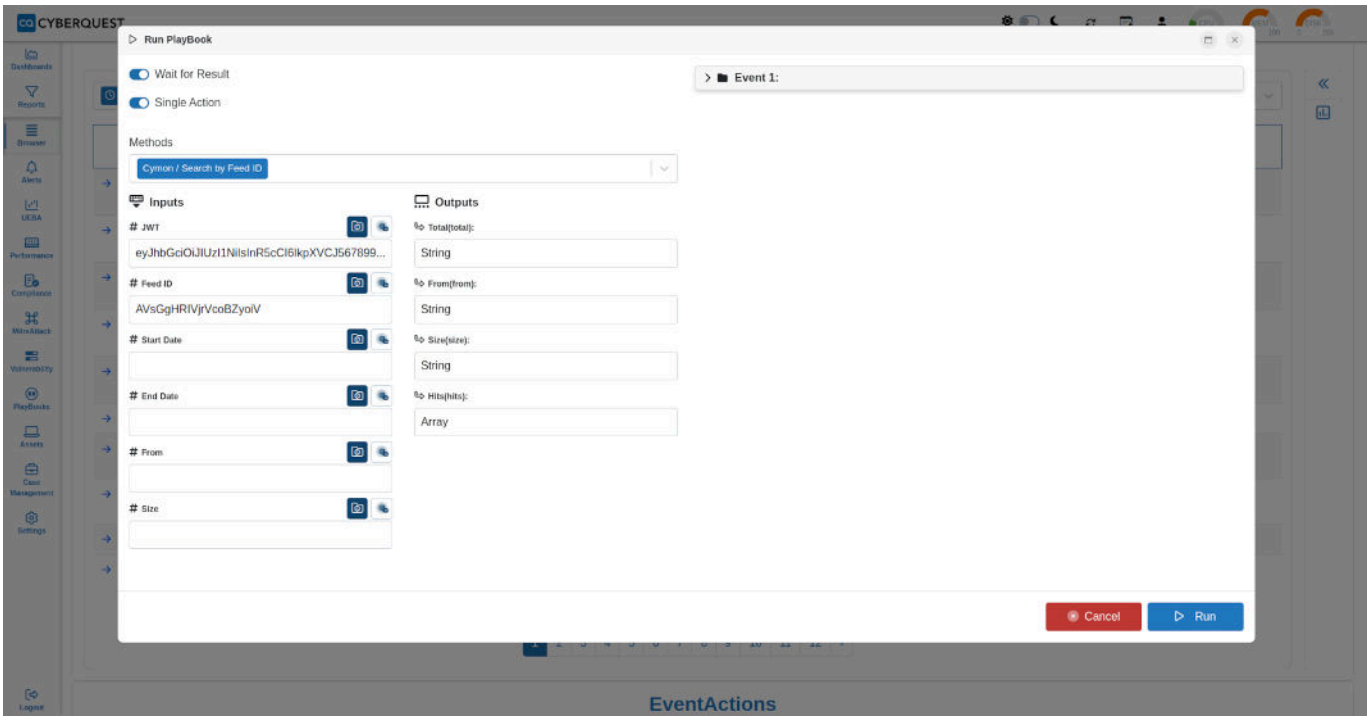


Inputs	Description
JWT (is required)	The JSON Web Token which was created previously (in Login)
Term (is required)	The query value (term) to search for
Start Date	The start date for searching
End Date	The end date for searching
From	The offset to use for pagination
Size	The limit to use for pagination

Outputs	Description
Total (total)	Total number of objects in database for query
From (from)	The query offset value
Size (size)	The query limit value for how many objects to return
Hits (hits)	The threat reports searched by IP address

Cymon/Search by Feed ID method

Get threat reports in a feed.

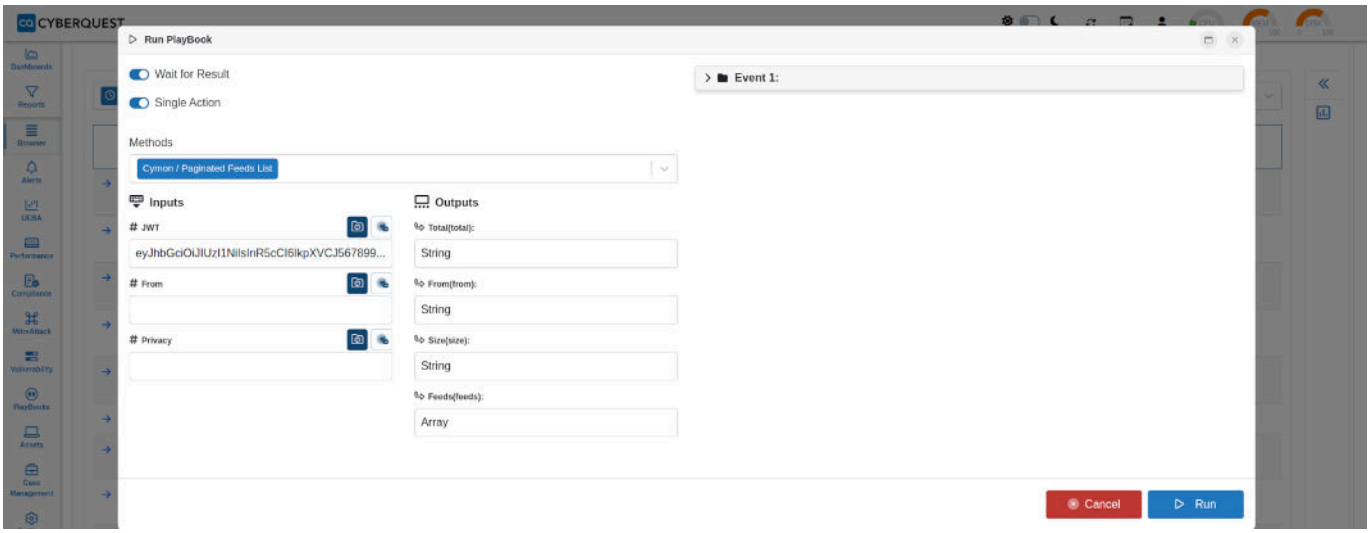


Inputs	Description
JWT (is required)	The JSON Web Token which was created previously (in Login)
Feed ID (is required)	The query value(Feed ID) to search for
Start Date	The start date for searching
End Date	The end date for searching
From	The offset to use for pagination
Size	The limit to use for pagination

Outputs	Description
Total (total)	Total number of objects in database for query
From (from)	The query offset value
Size (size)	The query limit value for how many objects to return
Hits (hits)	The threat reports searched by IP address

Cymon/Paginated Feeds List method

Get paginated list of feeds.

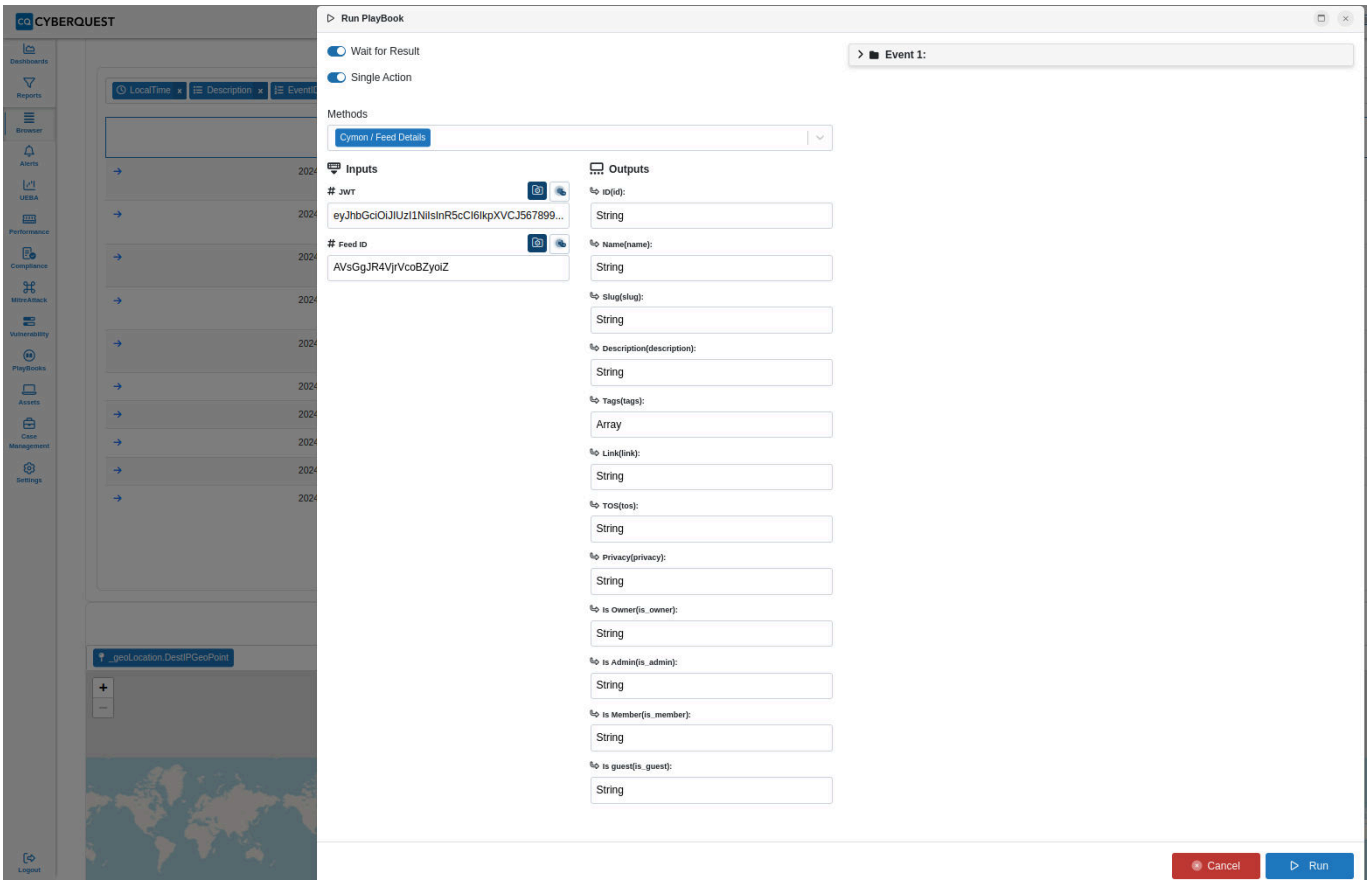


Inputs	Description
JWT (is required)	The JSON Web Token which was created previously (in Login)
From	The offset to use for pagination
Privacy	Return list of private or public feeds

Outputs	Description
Total (total)	Total number of objects in database for query
From (from)	The query offset value
Size (size)	The query limit value for how many objects to return
Feeds (feeds)	A list of searched feeds

Cymon/Feed Details method

Get feed object.

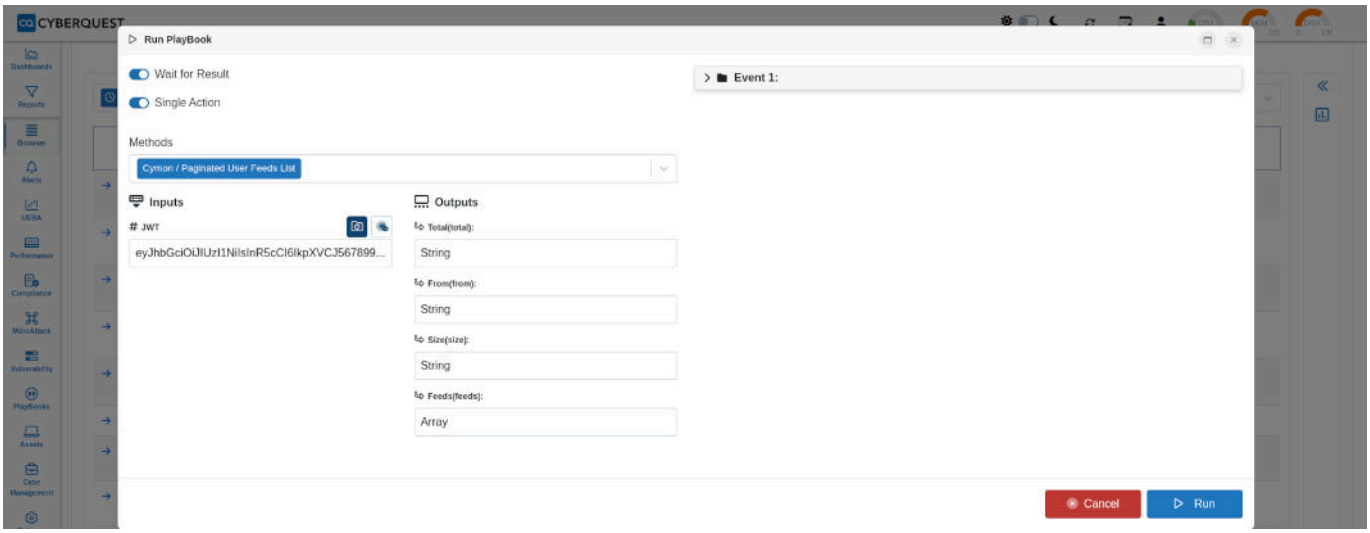


Inputs	Description
JWT (is required)	The JSON Web Token which was created previously (in Login)
Feed ID (is required)	ID of the Feed

Outputs	Description
ID (id)	Feed ID
Name (name)	Feed name
Slug (slug)	URL-friendly slug
Description (description)	Feed description tex
Tags (tags)	List of tags to categorize and help others find this feed
Link (link)	URL for blog or website where users can learn more about this feed
TOS (tos)	Terms of Use for this feed
Privacy (privacy)	Can be set to either private or public (default)
Is Owner (is_owner)	Boolean indicating if current user owns this feed
Is Admin (is_admin)	Boolean indicating if current user can administer this feed
Is Member (is_member)	Boolean indicating if current user can contribute to this fee
Is guest (is_guest)	Boolean indicating if current user can read from this feed

Cymon/Paginated User Feeds List method

Get paginated list of feeds that user has access to.

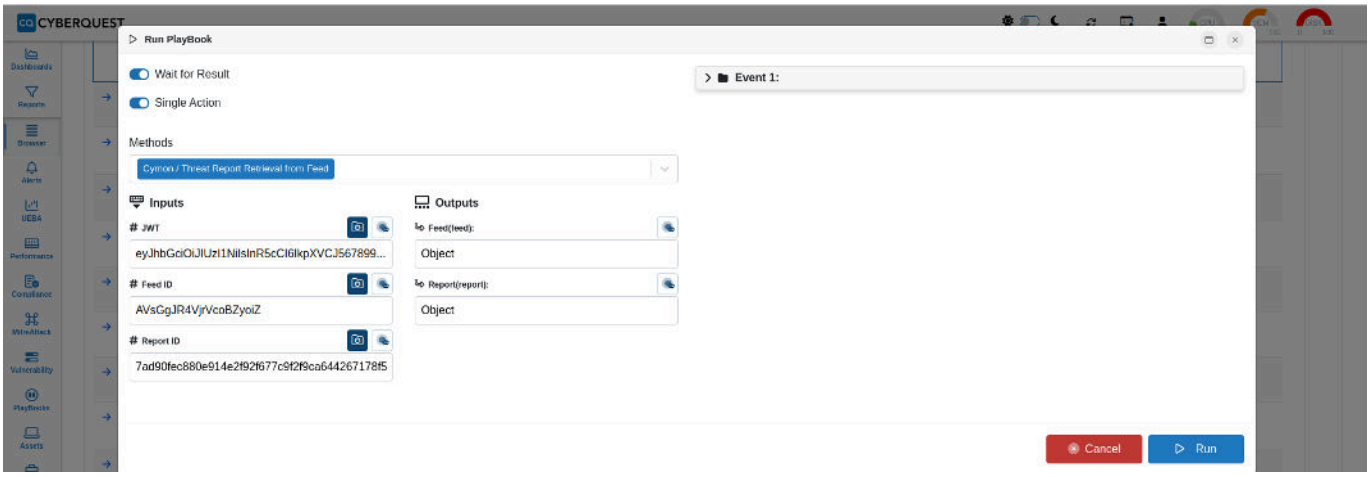


Inputs	Description
JWT (is required)	The JSON Web Token which was created previously (in Login)

Outputs	Description
Total (total)	Total number of objects in database for query
From (from)	The query offset value
Size (size)	The query limit value for how many objects to return
Feeds (feeds)	A list of searched feeds

Cymon/Threat Report Retrieval from Feed method

Get threat report from feed.

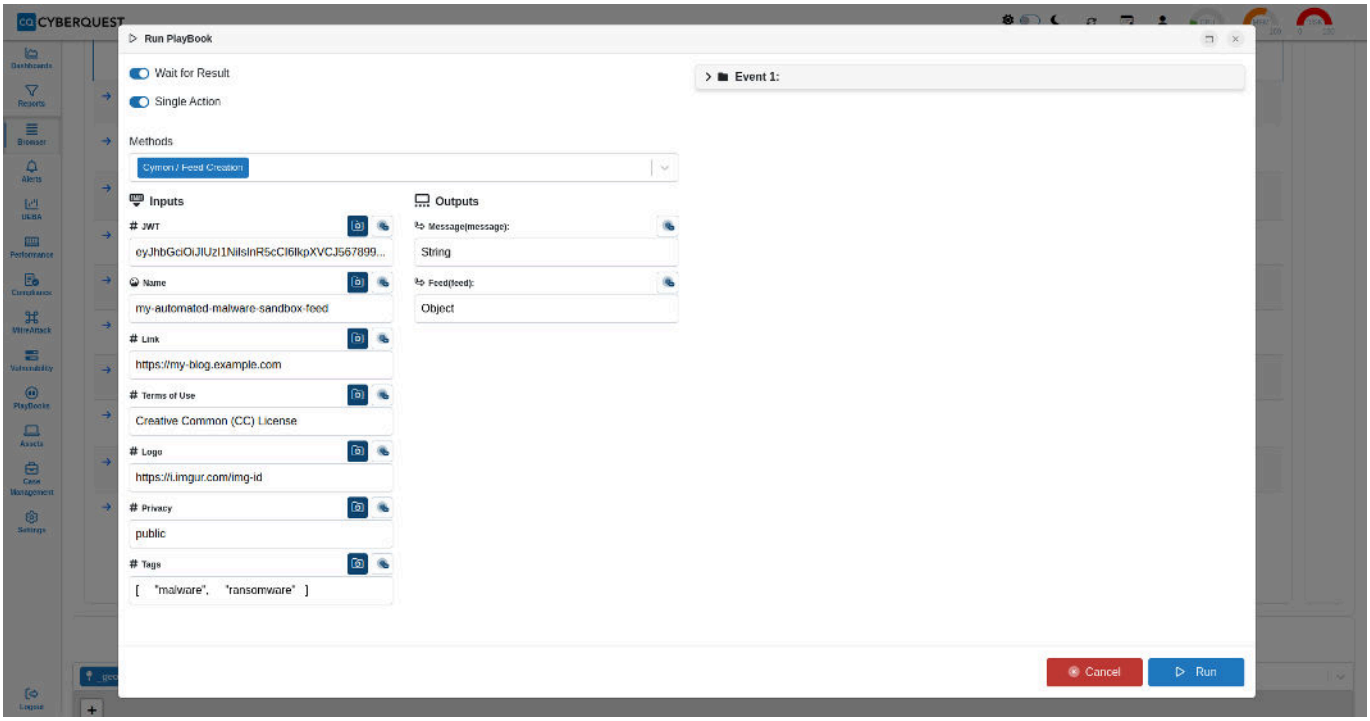


Inputs	Description
JWT (is required)	The JSON Web Token which was created previously (in Login)
Feed ID (is required)	ID of the Feed
Report ID (is required)	ID of the report

Outputs	Description
Feed (feed)	Feed details
Report (report)	The reports from feed

Cymon/Feed Creation method

Create a new feed for threat reports.

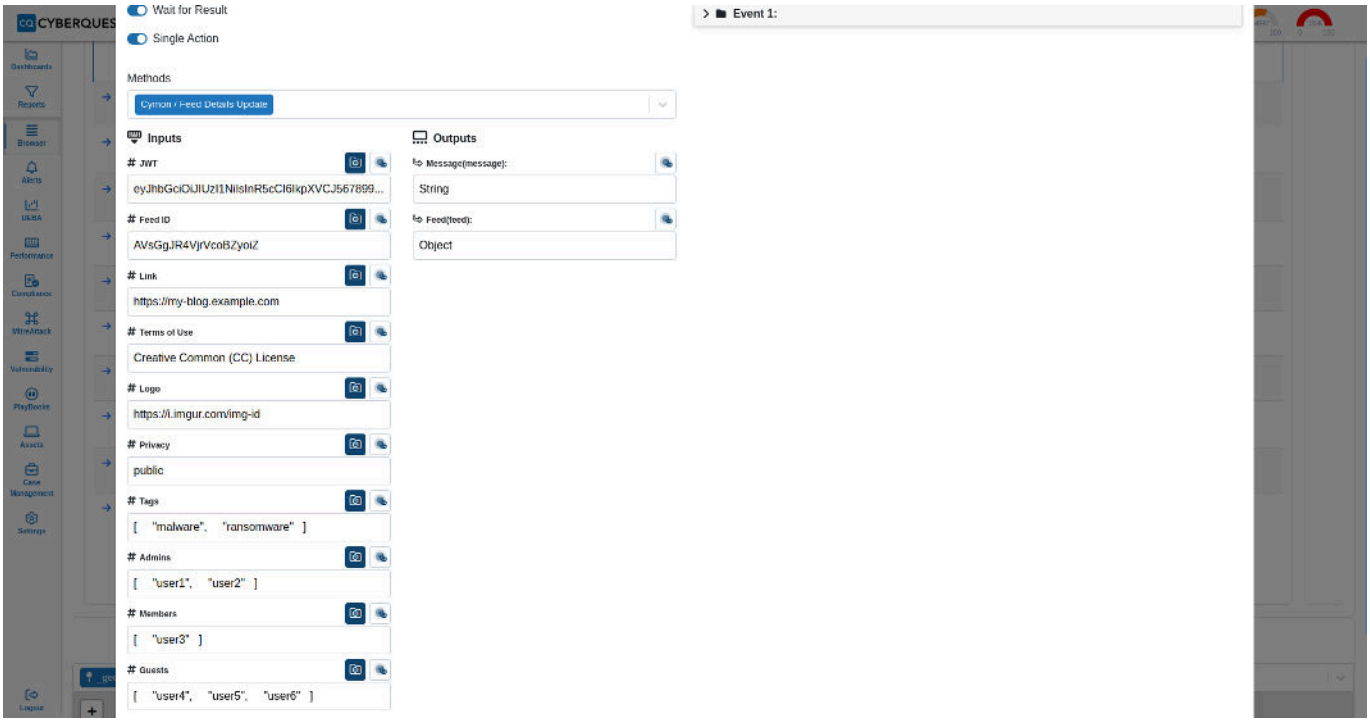


Inputs	Description
JWT (is required)	The JSON Web Token which was created previously (in Login)
Name (is required)	Feed name
Link (is required)	URL for blog or website where users can learn more about this feed
Terms of Use	Terms of Use for this feed
Logo	URL for small thumbnail for this feed (must be hosted on imgur CDN)
Privacy (is required)	Can be set to either private or public (default)
Tags	List of tags to categorize and help others find this feed

Outputs	Description
Message (message)	Success message
Feed (feed)	Feed details

Cymon/Feed Details Update method

Update details of an existing feed.

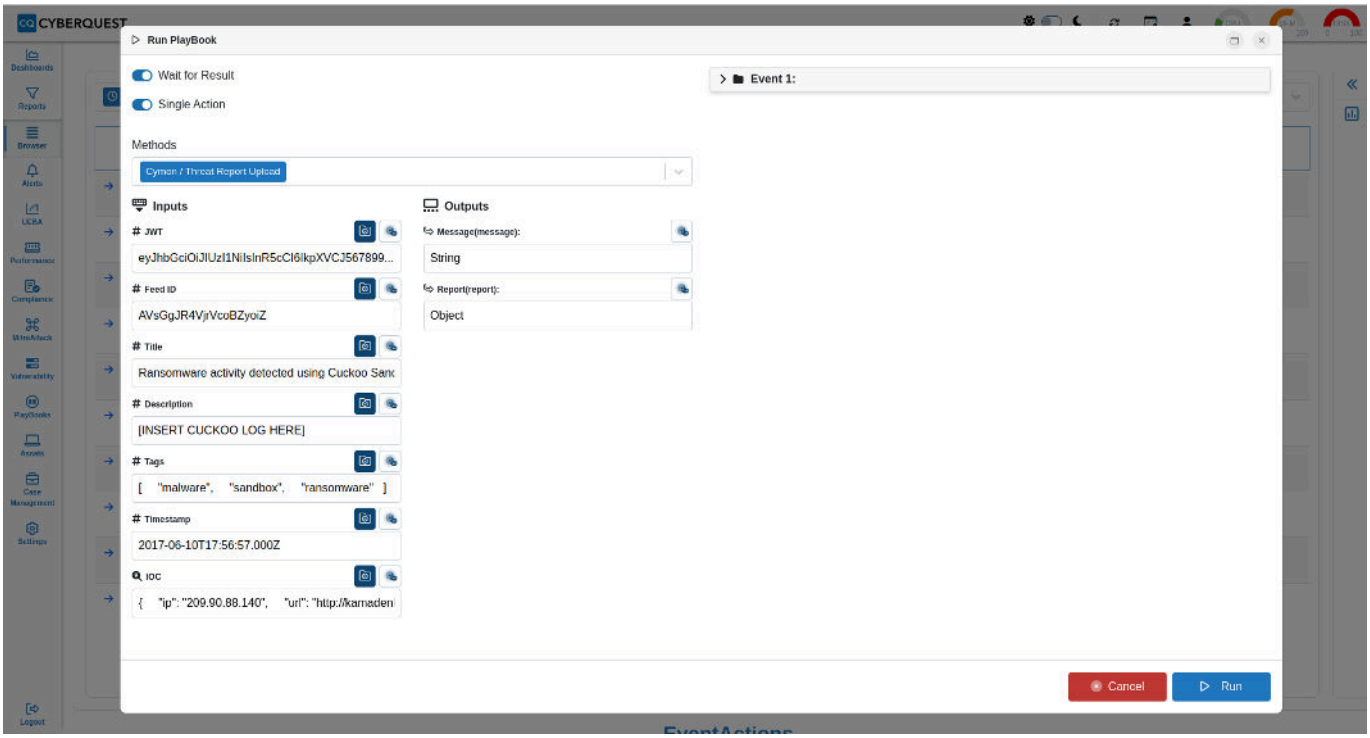


Inputs	Description
JWT (is required)	The JSON Web Token which was created previously (in Login)
Feed ID (is required)	The ID of the Feed which will be updated
Link	URL for blog or website where users can learn more about this feed
Terms of Use	Terms of Use for this feed
Logo	URL for small thumbnail for this feed (must be hosted on imgur CDN)
Privacy	Can be set to either private or public (default)
Tags	List of tags to categorize and help others find this feed
Admins	List of usernames that have update, post, and read permissions to this feed
Members	List of usernames that have post and read permissions to this feed
Guests	List of usernames that have read permission to this feed

Outputs	Description
Message (message)	Success message
Feed (feed)	Feed details

Cymon/Threat Report Upload method

Upload a threat report with observables.

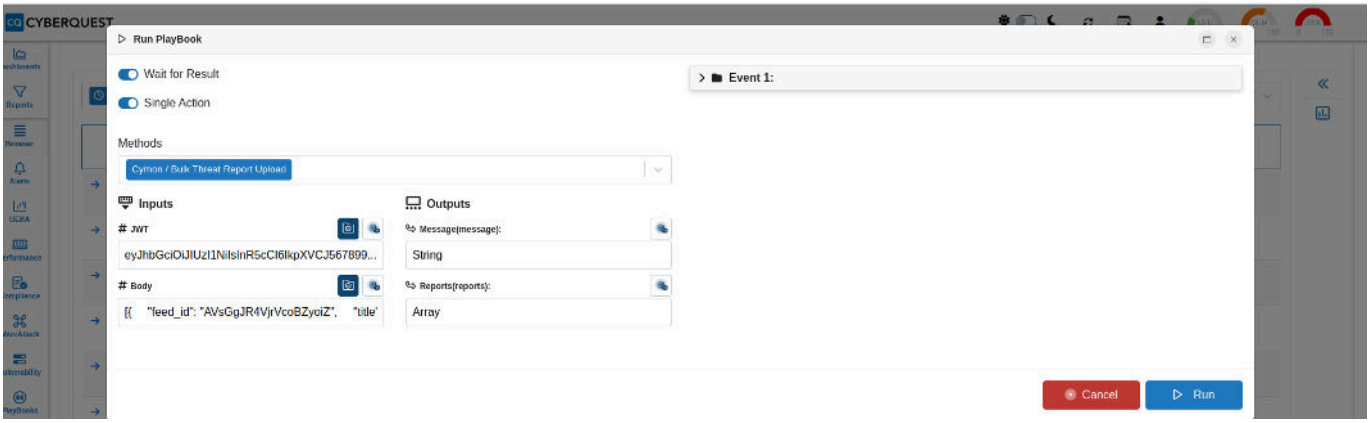


Inputs	Description
JWT (is required)	The JSON Web Token which was created previously (in Login)
Feed ID	The Feed ID to post this report in
Title	Short report title
Description	Long technical description
Tags	List of tags to categorize and help others find this report
Timestamp	An ISO8601 date string for when this IoC was observed
IP	IPv4 or IPv6
URL	Malicious URL indicator
Hostname	Domain with all subdomains
Domain	Root domain
MD5	MD5 hash of a malicious binary
SHA1	SHA1 hash of a malicious binary
SHA256	SHA256 hash of a malicious binary
SSDEEP	SSDEEP hash of a malicious binary

Outputs	Description
Message (message)	Success message.
Report (report)	Details about submitted report

Cymon/Bulk Threat Report Upload method

Upload multiple threat reports in one request.



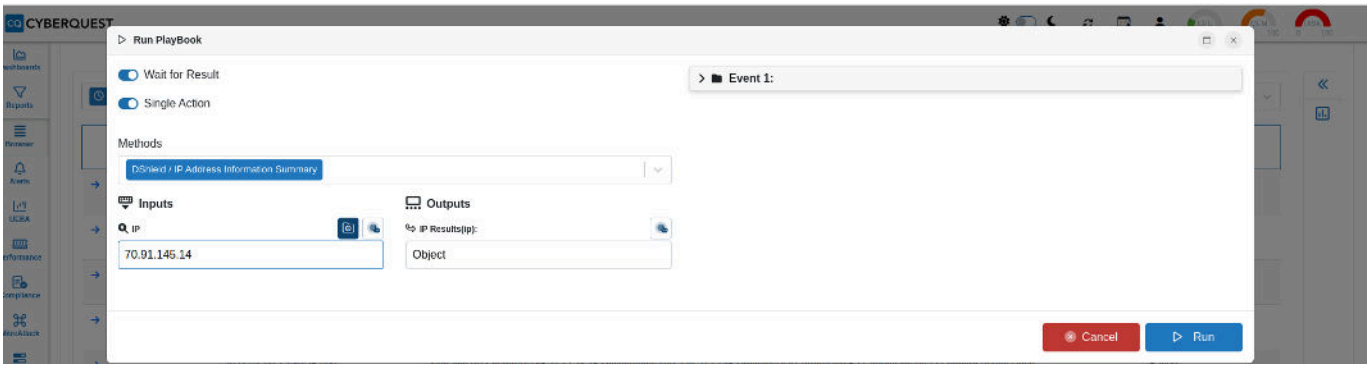
Inputs	Description
JWT (is required)	The JSON Web Token which was created previously (in Login)
Body (is required)	The body of this method

Outputs	Description
Message(message)	Success message
Reports(reports)	Details of submitted reports

DShield

DShield/IP Address Information Summary method

Returns a summary of the information our database holds for a particular IP address.

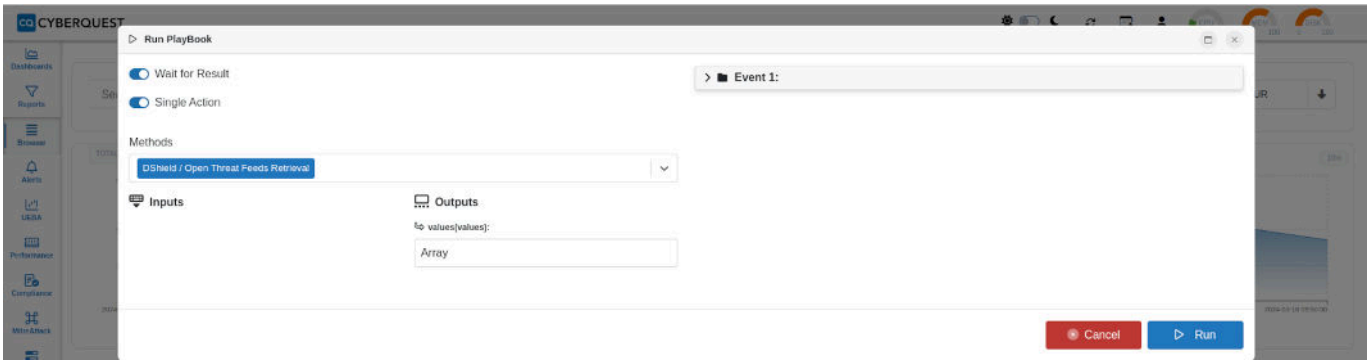


Inputs	Description
IP (is required)	The IP that is being searched

Outputs	Description
IP Results(ip)	The results of the API call

DShield/Open Threat Feeds Retrieval method

The DShield server is the source of retrieval for open threat feeds.

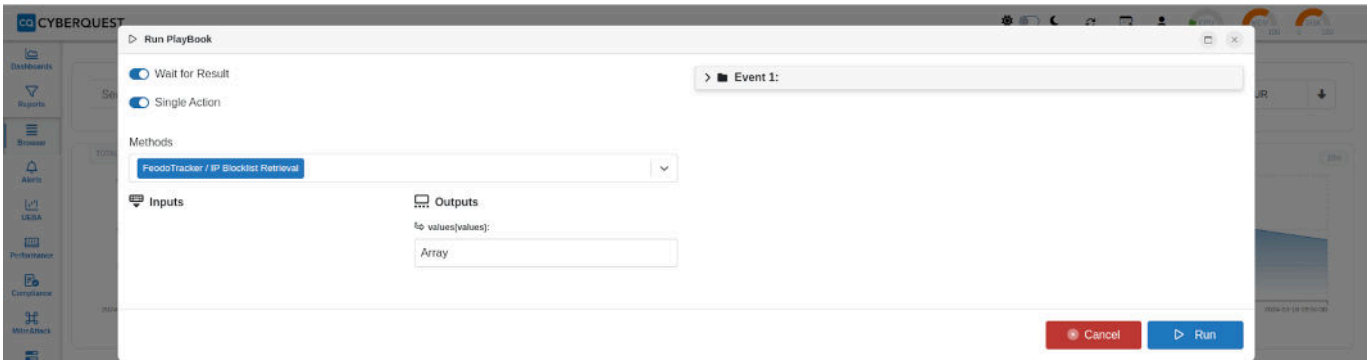


Outputs	Description
values(values)	The results of the API call

Feodo Tracker

FeodoTracker/IP Blocklist Retrieval method

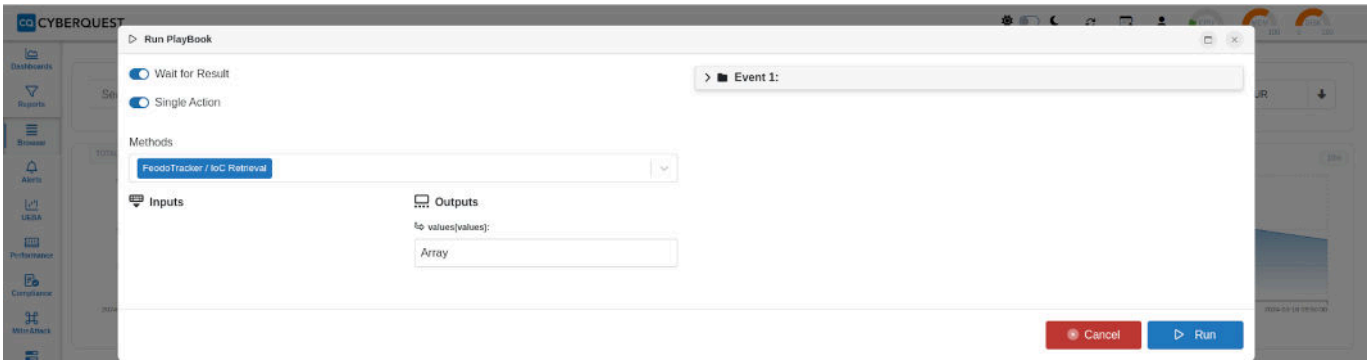
Get IP Blocklist.



Outputs	Description
values(values)	The results of the API call

FeodoTracker/IoC Retrieval method

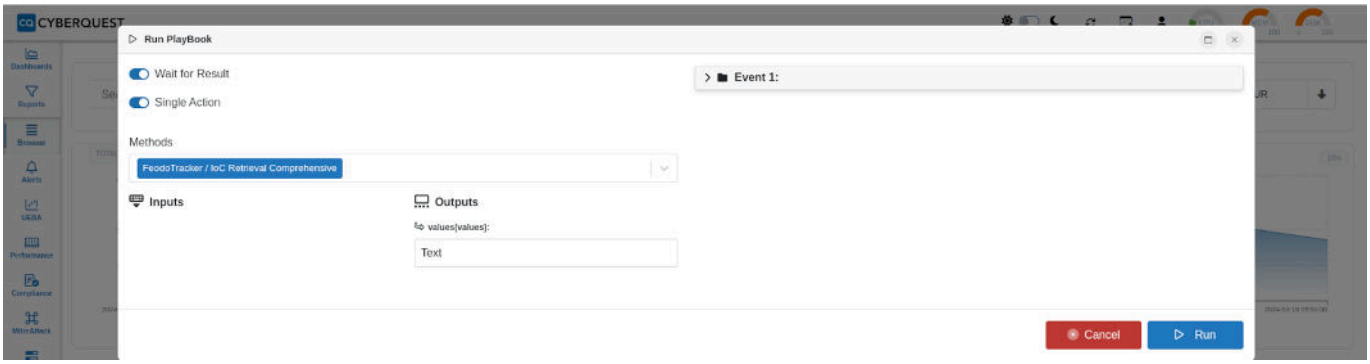
Get Indicators of Compromise(IOC).



Outputs	Description
values(values)	The results of the API call

FeodoTracker/IoC Retrieval Comprehensive method

Feodo Tracker provides a comprehensive list of botnet C2s ever detected. However, due to IP address recycling, there is a higher risk of false positives in this dataset.

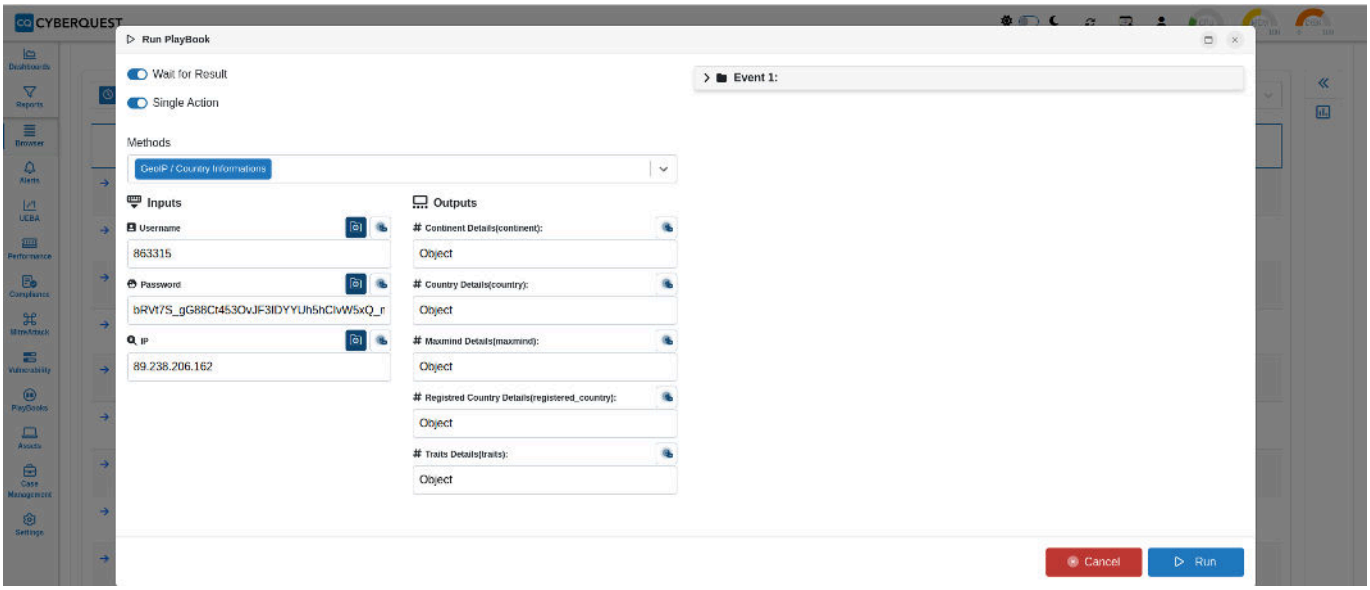


Outputs	Description
values(values)	The results of the API call

GeoIP

GeoIP/Country Informations method

Receives information about the country of the entered IP.

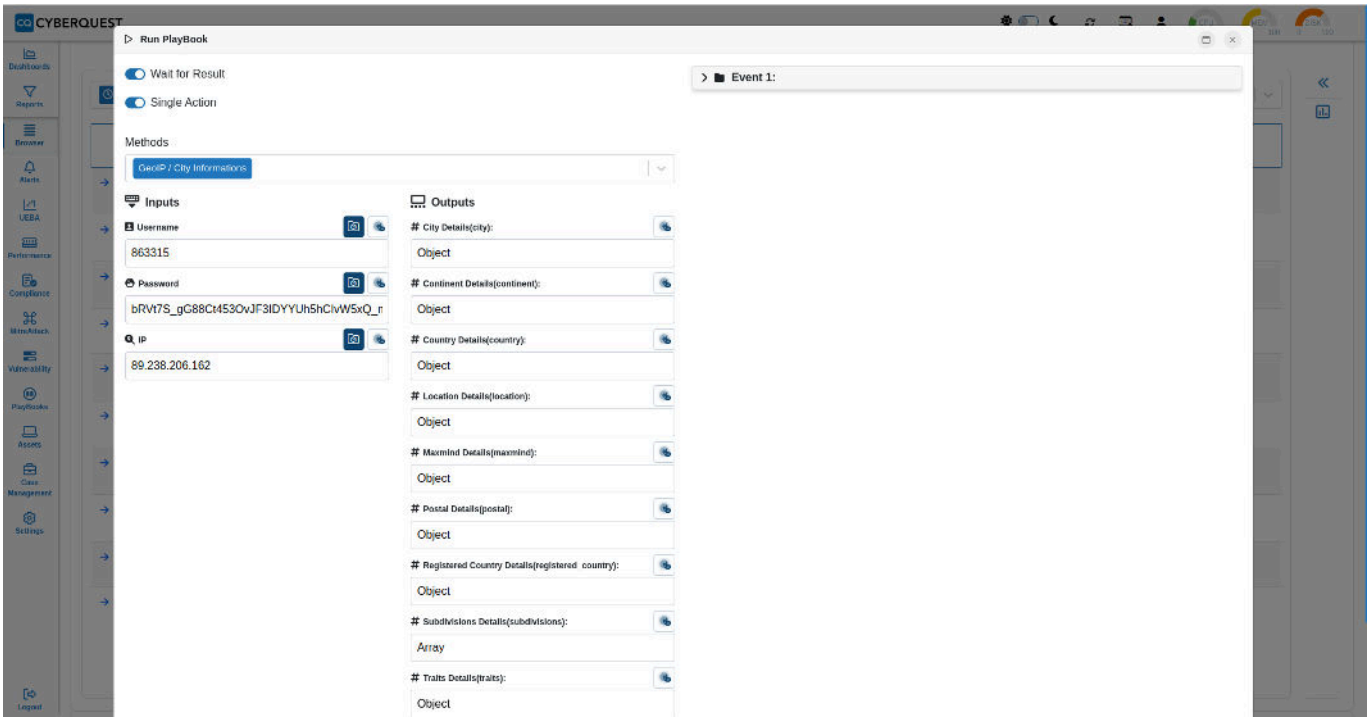


Inputs	Description
Username (is required)	To use this API you must have an account on Maxmind
Password (is required)	To use this API you must have an account on Maxmind
IP (is required)	The investigated IP

Outputs	Description
Continent Details(continent)	A JSON object containing information about the continent associated with the IP address.
Country Details(country)	A JSON object containing details about the country where MaxMind believes the end user is located
Maxmind Details(maxmind)	A JSON object containing information related to your MaxMind account
Registered Country Details(registered_country)	A JSON object containing details about the country in which the ISP has registered the IP address
Traits Details(traits)	A JSON object containing general traits associated with the IP address

GeoIP/City Informations method

Receives information about the city of the entered IP.

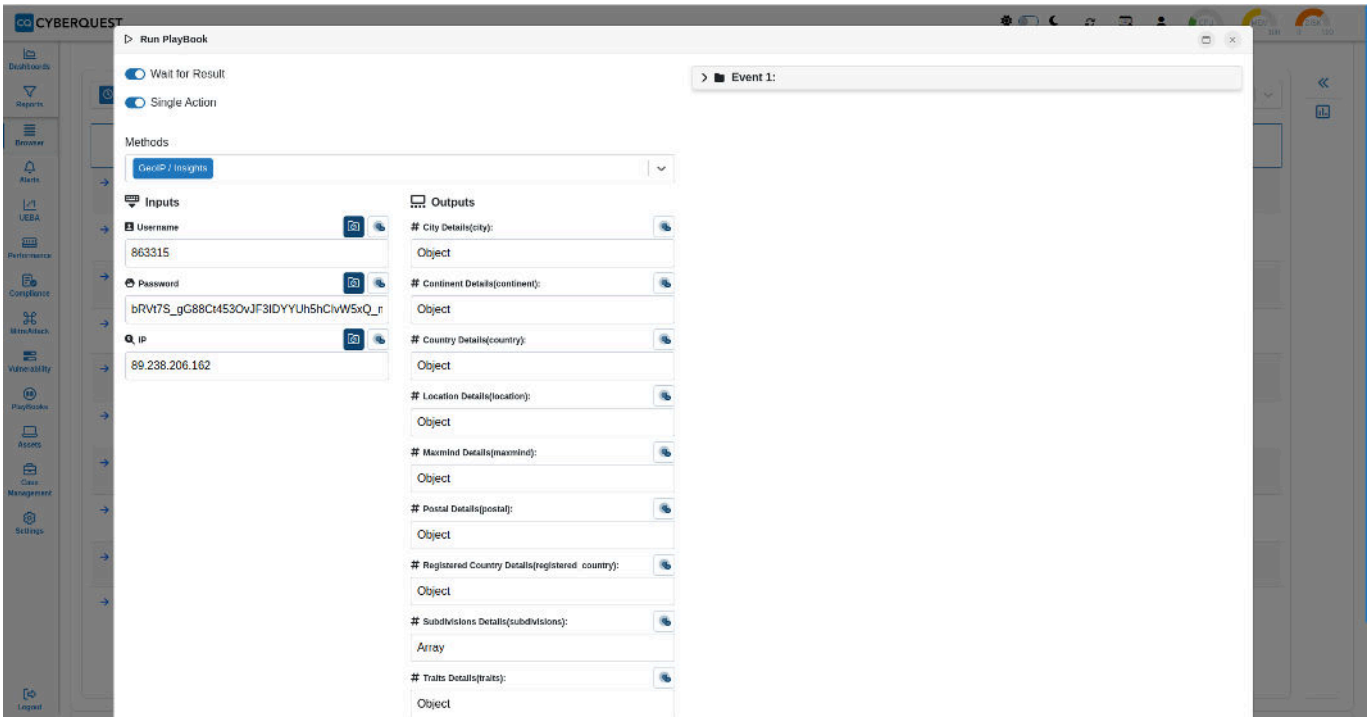


Inputs	Description
Username (is required)	To use this API you must have an account on Maxmind
Password (is required)	To use this API you must have an account on Maxmind
IP (is required)	The investigated IP

Outputs	Description
City Details(city)	A JSON object containing details about the city associated with the IP address
Continent Details(continent)	A JSON object containing information about the continent associated with the IP address.
Country Details(country)	A JSON object containing details about the country where MaxMind believes the end user is located
Location Details(location)	A JSON object containing specific details about the location associated with the IP address
Maxmind Details(maxmind)	A JSON object containing information related to your MaxMind account
Postal Details(postal)	A JSON object containing details about the postal code associated with the IP address
Registered Country Details(registered_country)	A JSON object containing details about the country in which the ISP has registered the IP address
Subdivisions Details(subdivisions)	An array of JSON objects. Each of these objects contains details about a subdivision of the country in which the IP address resides. Subdivisions are arranged from largest to smallest. For instance, the response for Oxford in the United Kingdom would have an object for England as the first element in subdivisions array and an object for Oxfordshire as the second element. The subdivisions array for Minneapolis in the United States will have a single object for Minnesota.
Traits Details(traits)	A JSON object containing general traits associated with the IP address

GeoIP/Insights method

Receives information about the insights of the entered IP.

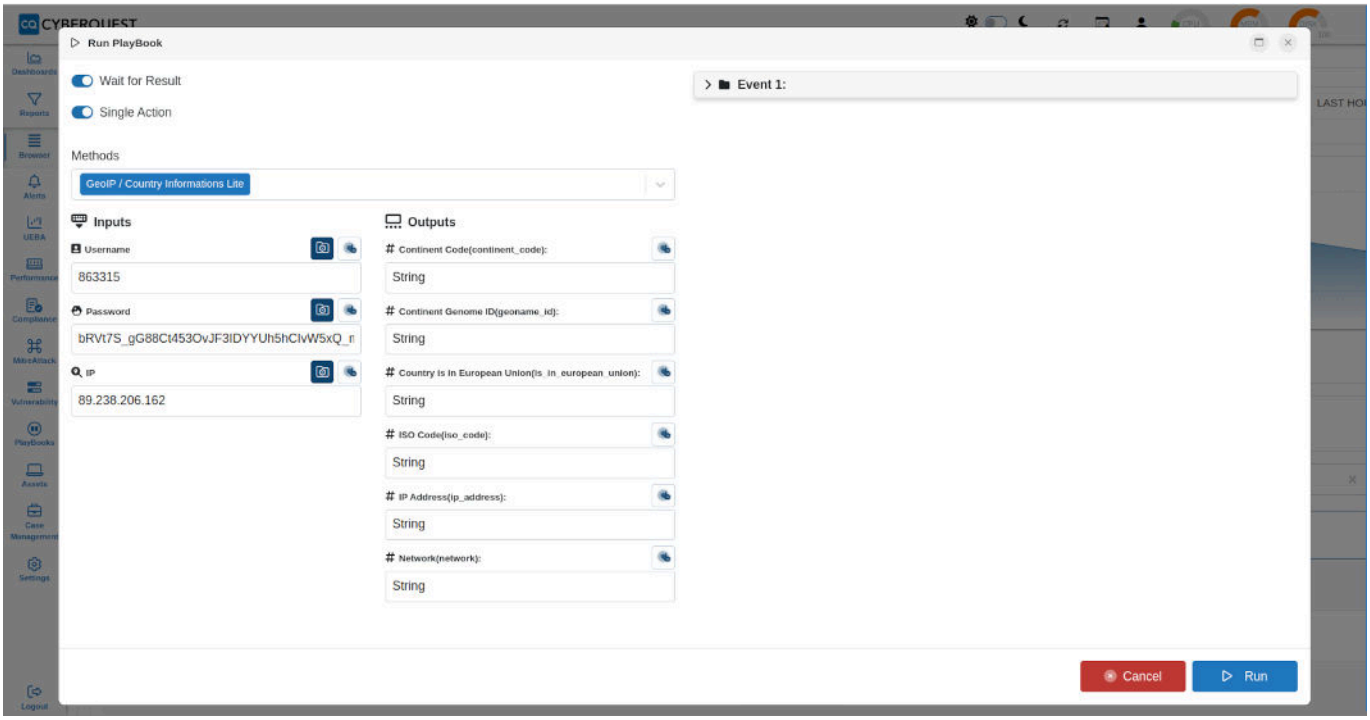


Inputs	Description
Username (is required)	To use this API you must have an account on Maxmind
Password (is required)	To use this API you must have an account on Maxmind
IP (is required)	The investigated IP

Outputs	Description
City Details(city)	A JSON object containing details about the city associated with the IP address
Continent Details(continent)	A JSON object containing information about the continent associated with the IP address
Country Details(country)	A JSON object containing details about the country where MaxMind believes the end user is located
Location Details(location)	A JSON object containing specific details about the location associated with the IP address
Maxmind Details(maxmind)	A JSON object containing information related to your MaxMind account
Postal Details(postal)	A JSON object containing details about the postal code associated with the IP address
Registered Country Details(registered_country)	A JSON object containing details about the country in which the ISP has registered the IP address
Subdivisions Details(subdivisions)	An array of JSON objects. Each of these objects contains details about a subdivision of the country in which the IP address resides. Subdivisions are arranged from largest to smallest. For instance, the response for Oxford in the United Kingdom would have an object for England as the first element in subdivisions array and an object for Oxfordshire as the second element. The subdivisions array for Minneapolis in the United States will have a single object for Minnesota.
Traits Details(traits)	A JSON object containing general traits associated with the IP address

GeoIP/Country Informations Lite method

Receives information about the country of the entered IP.

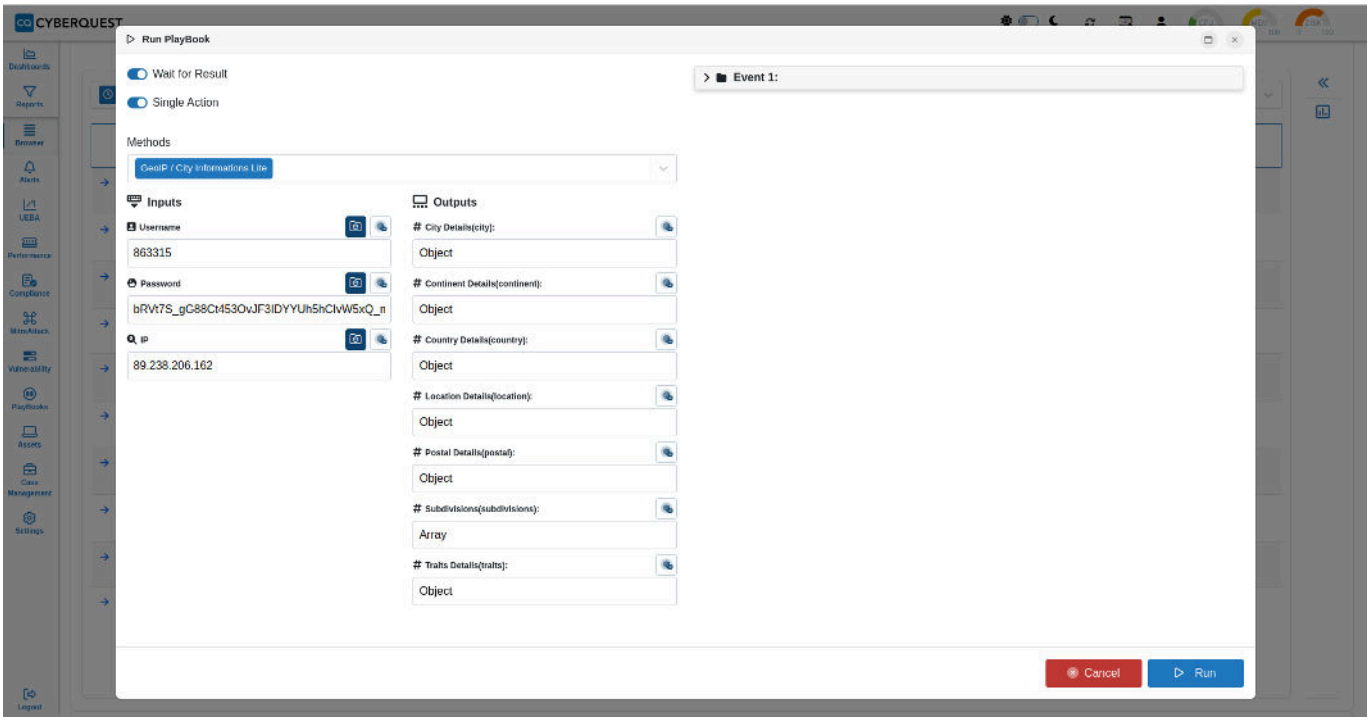


Inputs	Description
Username (is required)	To use this API you must have an account on Maxmind
Password (is required)	To use this API you must have an account on Maxmind
IP (is required)	The investigated IP

Outputs	Description
Continent Details(continent)	A JSON object containing information about the continent associated with the IP address
Country Details(country)	A JSON object containing details about the country where MaxMind believes the end user is located
Registered Country Details(registered_country)	A JSON object containing details about the country in which the ISP has registered the IP address
Traits Details(traits)	A JSON object containing general traits associated with the IP address

GeoIP/City Informations Lite method

Receives information about the city of the entered IP.



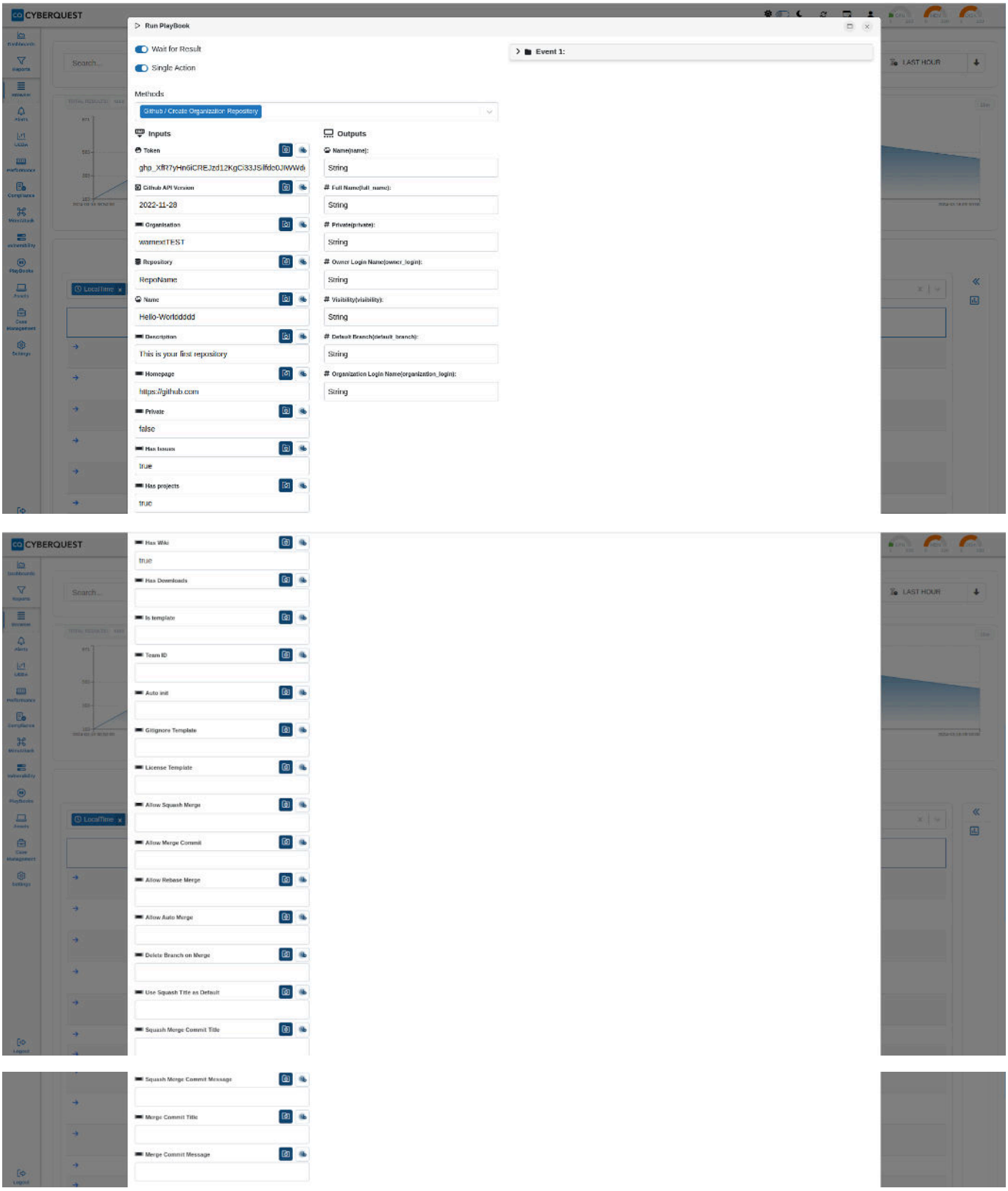
Inputs	Description
Username (is required)	To use this API you must have an account on Maxmind
Password (is required)	To use this API you must have an account on Maxmind
IP (is required)	The investigated IP

Outputs	Description
City Details(city)	A JSON object containing details about the city associated with the IP address
Continent Details(continent)	A JSON object containing information about the continent associated with the IP address
Country Details(country)	A JSON object containing details about the country where MaxMind believes the end user is located
Location Details(location)	A JSON object containing specific details about the location associated with the IP address
Maxmind Details(maxmind)	A JSON object containing information related to your MaxMind account
Postal Details(postal)	A JSON object containing details about the postal code associated with the IP address
Registered Country Details(registered_country)	A JSON object containing details about the country in which the ISP has registered the IP address
Subdivisions Details(subdivisions)	An array of JSON objects. Each of these objects contains details about a subdivision of the country in which the IP address resides. Subdivisions are arranged from largest to smallest. For instance, the response for Oxford in the United Kingdom would have an object for England as the first element in subdivisions array and an object for Oxfordshire as the second element. The subdivisions array for Minneapolis in the United States will have a single object for Minnesota.
Traits Details(traits)	A JSON object containing general traits associated with the IP address

Github

Github/Create Organization Repository method

Creates a new repository in the specified organization. The authenticated user must be a member of the organization.

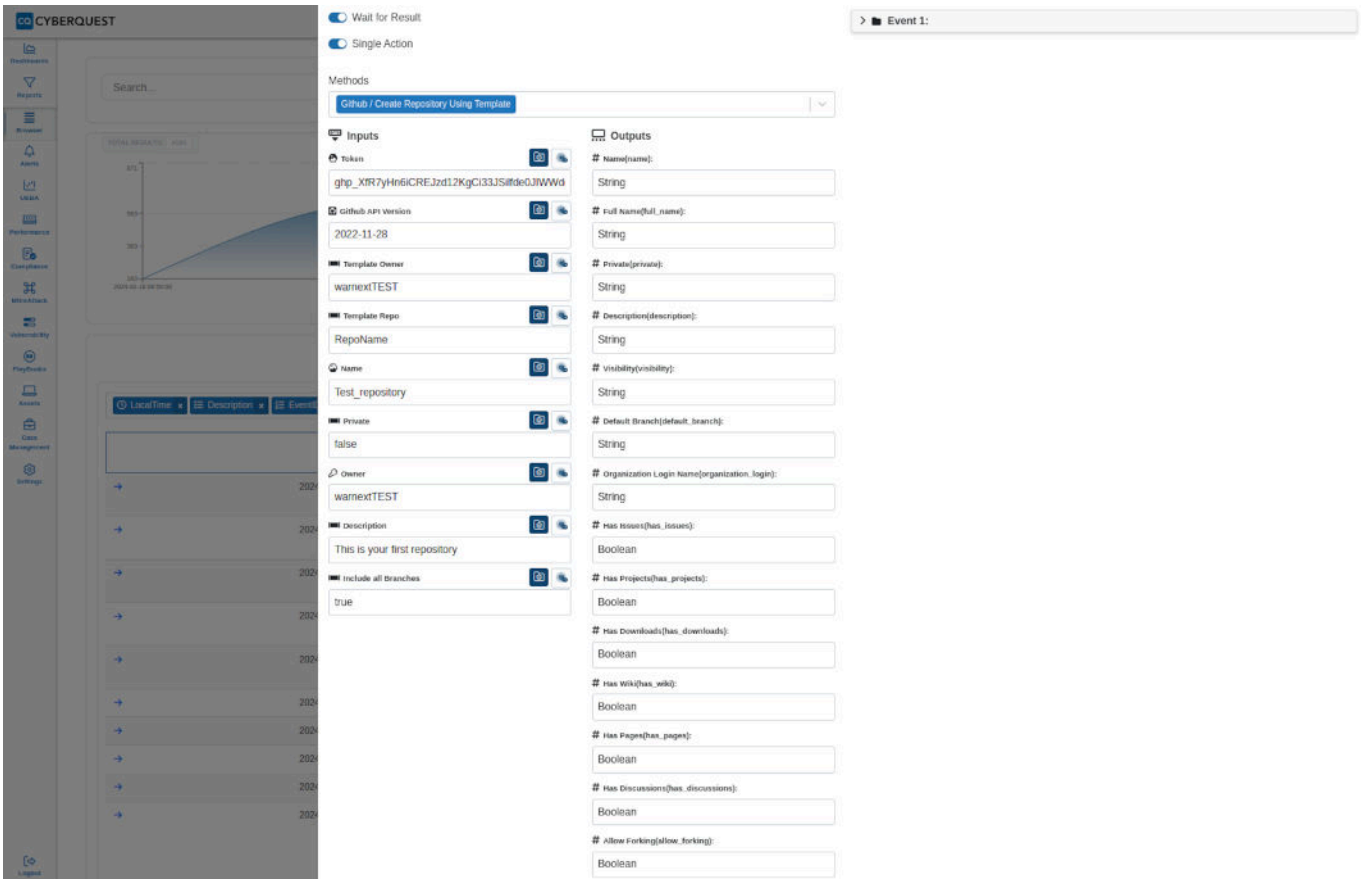

CYBERQUEST
Run PlayBook
Wait for Result
Single Action
Methods
Github / Create Organization Repository
Inputs
Token
Github API Version
2022-11-28
Organisation
wamextTEST
Repository
RepoName
Name
Hello-Worlddddd
Description
This is your first repository
Homepage
https://github.com
Private
false
Has Issues
true
Has projects
true
Has Wiki
true
Has Downloads
Is template
Team ID
Auto init
Gitignore Template
License Template
Allow Squash Merge
Allow Merge Commit
Allow Rebase Merge
Allow Auto Merge
Delete Branch on Merge
Use Squash Title as Default
Squash Merge Commit Title
Squash Merge Commit Message
Merge Commit Title
Merge Commit Message
Outputs
Name(name):
String
Full Name(full_name):
String
Private(private):
String
Owner Login Name(owner_login):
String
Visibility(visibility):
String
Default Branch(default_branch):
String
Organization Login Name(organization_login):
String
Event 1:
LAST HOUR

Inputs	Description
Token (is required)	To use the Github API, you must have an API key
Github API Version (is required)	This parameter it is used to specify the version of the GitHub API being utilized
Organisation (is required)	The account owner of the repository
Repository (is required)	The name of the repository without the .git extension
Name (is required)	The name of the repository
Description	A short description of the repository
Homepage	The organization name. The name is not case sensitive.
Private	Whether the repository is private
Has Issues	Either true to enable issues for this repository or false to disable them
Has projects	Either true to enable projects for this repository or false to disable them. Note: If youre creating a repository in an organization that has disabled repository projects, the default is false, and if you pass true, the API returns an error
Has Wiki	Either true to enable the wiki for this repository or false to disable it
Has Downloads	Whether downloads are enabled
Is template	Either true to make this repo available as a template repository or false to prevent it
Team ID	The id of the team that will be granted access to this repository. This is only valid when creating a repository in an organization
Auto init	Pass true to create an initial commit with empty README
Gitignore Template	Desired language or platform .gitignore template to apply
License Template	Choose an open source license template that best suits your needs
Allow Squash Merge	Either true to allow squash-merging pull requests, or false to prevent squash-merging
Allow Merge Commit	Either true to allow merging pull requests with a merge commit, or false to prevent merging pull requests with merge commits
Allow Rebase Merge	Either true to allow rebase-merging pull requests, or false to prevent rebase-merging
Allow Auto Merge	Either true to allow auto-merge on pull requests, or false to disallow auto-merge
Delete Branch on Merge	Either true to allow automatically deleting head branches when pull requests are merged, or false to prevent automatic deletion. The authenticated user must be an organization owner to set this property to true
Use Squash Title as Default	Either true to allow squash-merge commits to use pull request title, or false to use commit message. **This property has been deprecated. Please use squash_merge_commit_title instead.
Squash Merge Commit Title	The default value for a squash merge commit title:PR_TITLE - default to the pull requests title.COMMIT_OR_PR_TITLE - default to the commits title (if only one commit) or the pull requests title (when more than one commit)
Squash Merge Commit Message	The default value for a squash merge commit message:PR_BODY - default to the pull requests body.COMMIT_MESSAGES - default to the branchs commit messages.BLANK - default to a blank commit messagE
Merge Commit Title	The default value for a merge commit title.PR_TITLE - default to the pull requests title.MERGE_MESSAGE - default to the classic title for a merge message (e.g., Merge pull request #123 from branch-name
Merge Commit Message	The default value for a merge commit message.PR_TITLE - default to the pull requests title.PR_BODY - default to the pull requests body.BLANK - default to a blank commit messagE

Outputs	Description
Name(name)	The name of the organization repository
Full Name(full_name)	The full name of the organization repository
Private(private)	True if the repository is private, otherwise is false
Owner Login Name(owner_login)	The owner login name
Visibility(visibility)	The visibility of the repository (public or private)
Default Branch(default_branch)	The name of the default branch
Organization Login Name(organization_login)	The organization login name

Github/Create Repository Using Template method

Creates a new repository using a repository template.

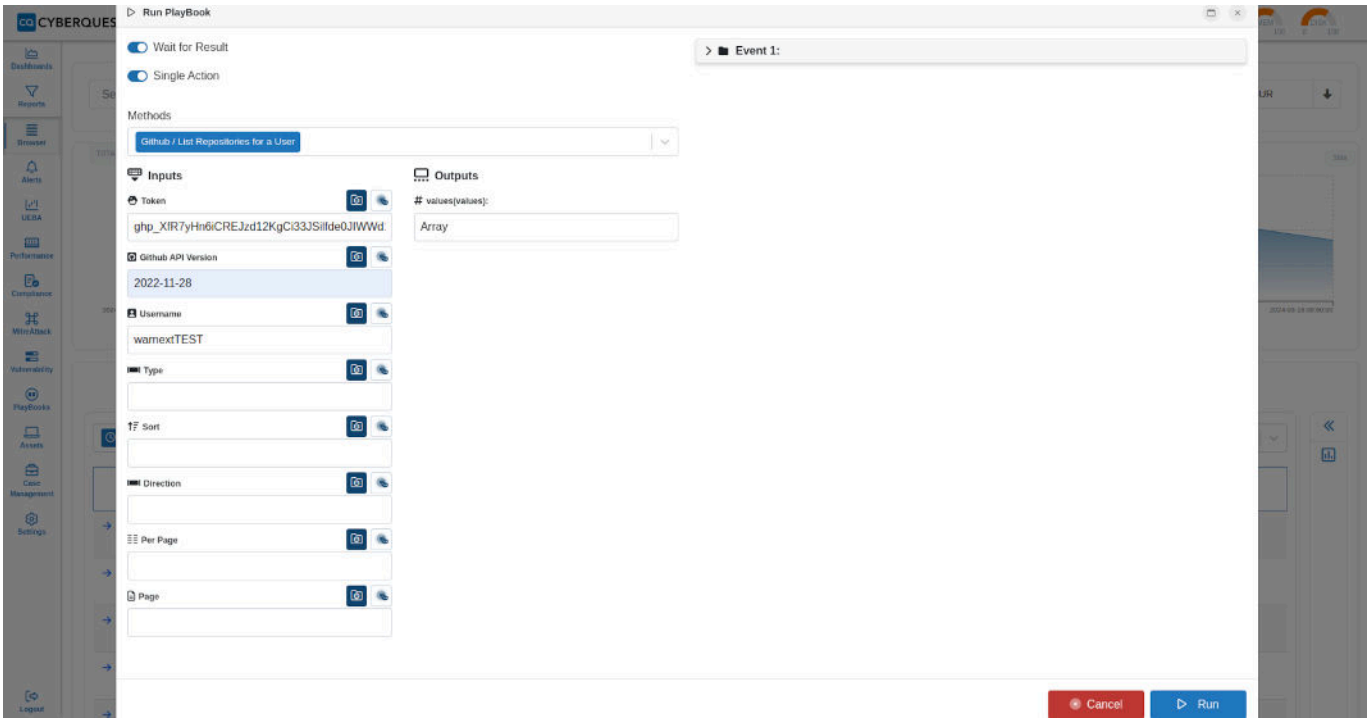


Inputs	Description
Token (is required)	To use the Github API, you must have an API key
Github API Version (is required)	This parameter it is used to specify the version of the GitHub API being utilized
Template Owner (is required)	The account owner of the template
Template Repo (is required)	The name of the repository without the .git extension
Name (is required)	The name of the repository
Private	Either true to create a new private repository or false to create a new public one
Owner	The organization or person who will own the new repository. To create a new repository in an organization, the authenticated user must be a member of the specified organization
Description	A short description of the new repository
Include all Branches	The name of the new repository

Outputs	Description
Name(name)	The name of repository template
Full Name(full_name)	The full name of repository template
Private(private)	True if the repository is private, otherwise is false
Description(description)	The description of the templetate repository
Visibility(visibility)	The visibility of the repository (public or private)
Default Branch(default_branch)	The name of the default branch
Organization Login Name(organization_login)	The organization login name
Has Issues(has_issues)	Either true to enable issues for this repository or false to disable them
Has Projects(has_projects)	Either true to enable projects for this repository or false to disable them. Note: If youre creating a repository in an organization that has disabled repository projects, the default is false, and if you pass true, the API returns an error
Has Downloads(has_downloads)	Whether downloads are enabled
Has Wiki(has_wiki)	Either true to enable the wiki for this repository or false to disable it
Has Pages(has_pages)	True if the repository has pages, otherwise false
Has Discussions(has_discussions)	True if the repository has discussions
Allow Forking(allow_forking)	True if the repository allows forking

Github/List Repositories for a User method

Lists public repositories for the specified user.

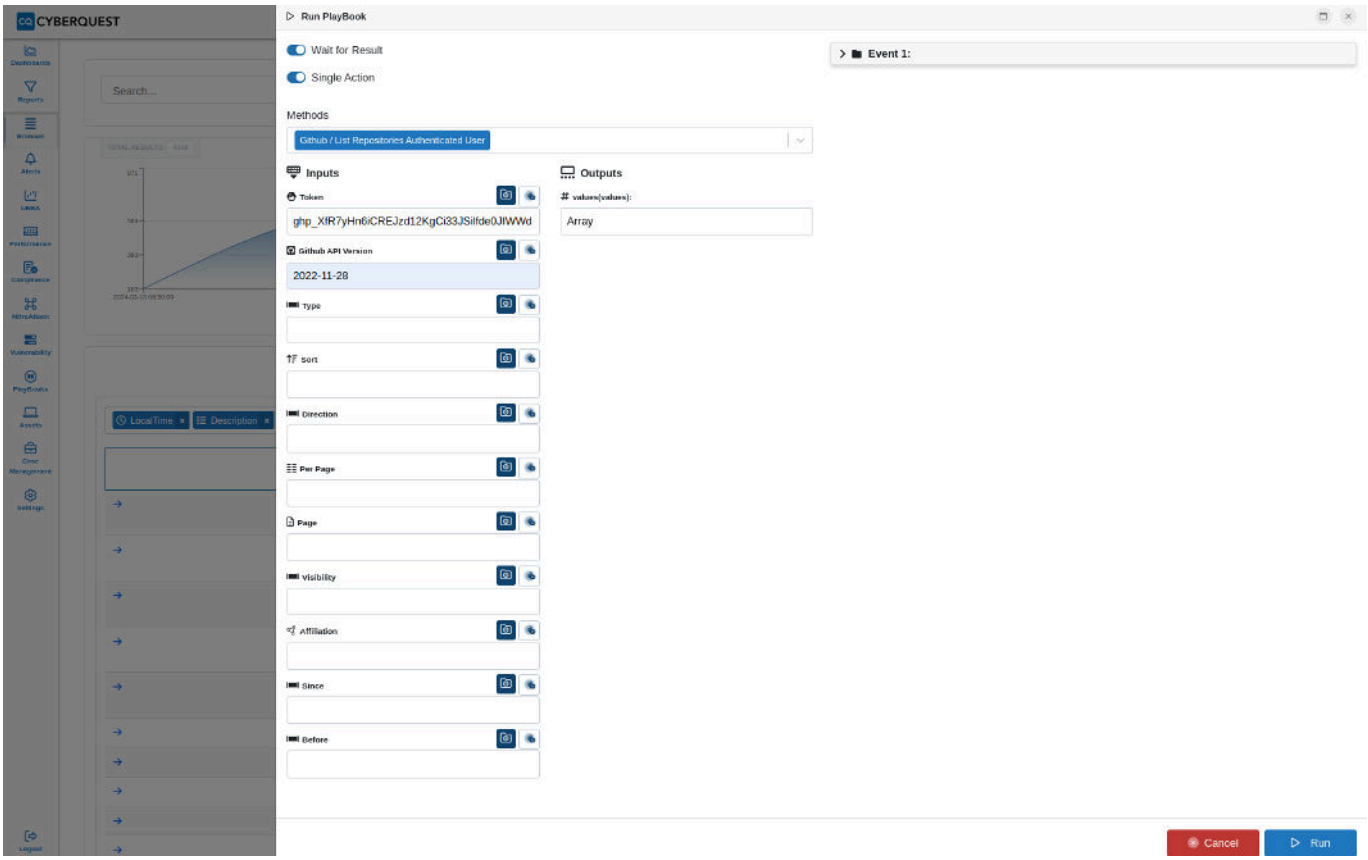


Inputs	Description
Token (is required)	To use the Github API, you must have an API key
Github API Version (is required)	This parameter it is used to specify the version of the GitHub API being utilized
Username (is required)	The handle for the GitHub user account
Type	Limit results to repositories of the specified type
Sort	The property to sort the results by
Direction	The order to sort by. Default: asc when using full_name, otherwise desc.
Per Page	The number of results per page (max 100)
Page	Page number of the results to fetch

Outputs	Description
values(values)	The results of the API call

Github/List Repositories Authenticated User method

Lists repositories that the authenticated user has explicit permission (:read, :write, or :admin) to access.

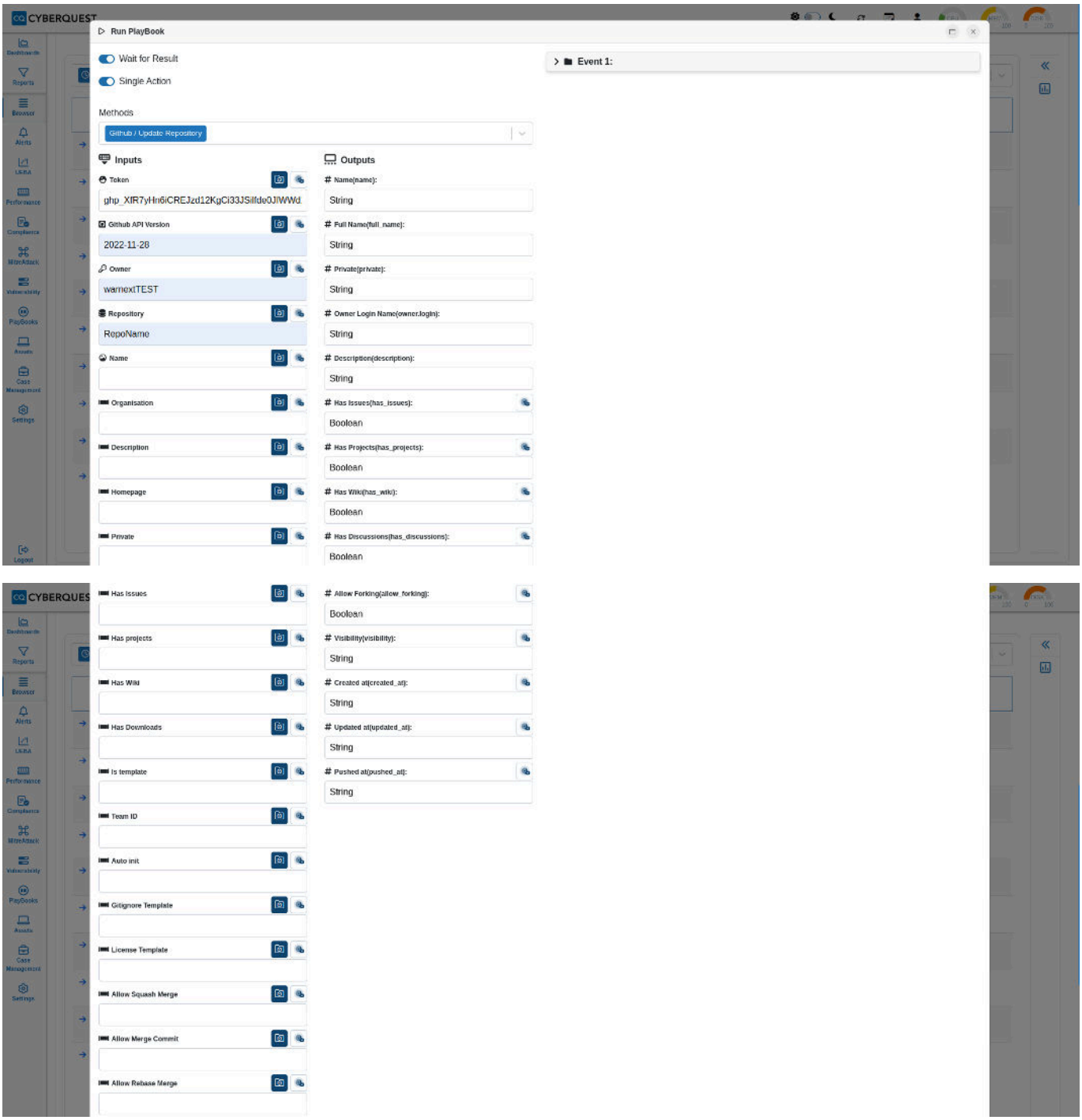


Inputs	Description
Token (is required)	To use the Github API, you must have an API key
Github API Version (is required)	This parameter it is used to specify the version of the GitHub API being utilized
Type	Limit results to repositories of the specified type
Sort	The property to sort the results by
Direction	The order to sort by. Default: asc when using full_name, otherwise desc.
Per Page	The number of results per page (max 100)
Page	Page number of the results to fetch
Visibility	Limit results to repositories with the specified visibility
Affiliation	Comma-separated list of values. Can include:owner: Repositories that are owned by the authenticated user.collaborator: Repositories that the user has been added to as a collaborator.organization_member: Repositories that the user has access to through being a member of an organization. This includes every repository on every team that the user is on
Since	Only show repositories updated after the given time
Before	Only show repositories updated before the given time

Outputs	Description
values(values)	The results of the API call

Github/Update Repository method

Update he repository given by user.


CYBERQUEST
Run PlayBook
Wait for Result
Single Action
Methods
Github / Update Repository
Inputs
Outputs
Event 1:
Token
ghp_XfR7yHn6iCREJzd12KgCi33JSilfde0JlWWd
Github API Version
2022-11-28
Owner
warnexITEST
Repository
RepoName
Name
Organisation
Description
Homepage
Private
Name(name):
String
Full Name(full_name):
String
Private(private):
String
Owner Login Name(owner.login):
String
Description(description):
String
Has Issues(has_issues):
Boolean
Has Projects(has_projects):
Boolean
Has Wiki(has_wiki):
Boolean
Has Discussions(has_discussions):
Boolean
Has Issues
Has projects
Has Wiki
Has Downloads
Is template
Team ID
Auto init
Gitignore Template
License Template
Allow Squash Merge
Allow Merge Commit
Allow Rebase Merge
Allow Forking(allow_forking):
Boolean
Visibility(visibility):
String
Created at(created_at):
String
Updated at(updated_at):
String
Pushed at(pushed_at):
String


Allow Auto Merge
Delete Branch on Merge
Use Squash Title as Default
Squash Merge Commit Title
Squash Merge Commit Message
Merge Commit Title
Merge Commit Message
Archived
Web Commit Sign off
Cancel
Run

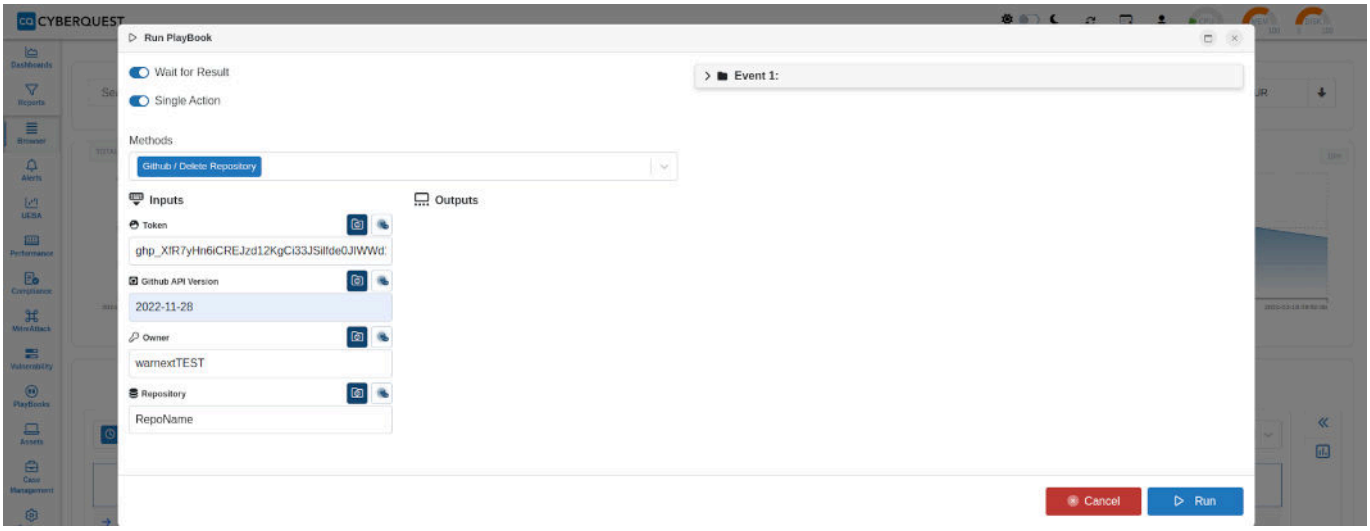
Inputs	Description
Token (is required)	To use the Github API, you must have an API key
Github API Version (is required)	This parameter it is used to specify the version of the GitHub API being utilized
Owner (is required)	The account owner of the repository
Repository (is required)	The name of the repository without the .git extension
Name	The name of the repository
Organisation	The organization name. The name is not case sensitive
Description	A short description of the repository
Homepage	The organization name. The name is not case sensitive
Private	Whether the repository is private
Has Issues	Either true to enable issues for this repository or false to disable them
Has projects	Either true to enable projects for this repository or false to disable them. Note: If youre creating a repository in an organization that has disabled repository projects, the default is false, and if you pass true, the API returns an error
Has Wiki	Either true to enable the wiki for this repository or false to disable it
Has Downloads	Whether downloads are enabled
Is template	Either true to make this repo available as a template repository or false to prevent it.
Team ID	The id of the team that will be granted access to this repository. This is only valid when creating a repository in an organization
Auto init	Pass true to create an initial commit with empty README
Gitignore Template	Desired language or platform .gitignore template to apply
License Template	Choose an open source license template that best suits your needs
Allow Squash Merge	Either true to allow squash-merging pull requests, or false to prevent squash-merging
Allow Merge Commit	Either true to allow merging pull requests with a merge commit, or false to prevent merging pull requests with merge commits
Allow Rebase Merge	Either true to allow rebase-merging pull requests, or false to prevent rebase-merging
Allow Auto Merge	Either true to allow auto-merge on pull requests, or false to disallow auto-merge
Delete Branch on Merge	Either true to allow automatically deleting head branches when pull requests are merged, or false to prevent automatic deletion. The authenticated user must be an organization owner to set this property to true
Use Squash Title as Default	Either true to allow squash-merge commits to use pull request title, or false to use commit message. **This property has been deprecated. Please use squash_merge_commit_title instead
Squash Merge Commit Title	The default value for a squash merge commit title:PR_TITLE - default to the pull requests title.COMMIT_OR_PR_TITLE - default to the commits title (if only one commit) or the pull requests title (when more than one commit)
Squash Merge Commit Message	The default value for a squash merge commit message:PR_BODY - default to the pull requests body.COMMIT_MESSAGES - default to the branchs commit messages.BLANK - default to a blank commit message
Merge Commit Title	The default value for a merge commit title.PR_TITLE - default to the pull requests title.MERGE_MESSAGE - default to the classic title for a merge message (e.g., Merge pull request #123 from branch-name)
Merge Commit Message	The default value for a merge commit message.PR_TITLE - default to the pull requests title.PR_BODY - default to the pull requests body.BLANK - default to a blank commit message
Archived	Whether to archive this repository. false will unarchive a previously archived repository

Inputs	Description
Web Commit Sign off	Either true to require contributors to sign off on web-based commits, or false to not require contributors to sign off on web-based commits

Outputs	Description
Name(name)	The name of the repository
Full Name(full_name)	The full name of repository
Private(private)	Whether the repository is private
Owner Login Name(owner.login)	The account owner of the repository
Description(description)	A short description of the repository
Has Issues(has_issues)	Either true to enable issues for this repository or false to disable them
Has Projects(has_projects)	Either true to enable projects for this repository or false to disable them. Note: If youre creating a repository in an organization that has disabled repository projects, the default is false, and if you pass true, the API returns an error
Has Wiki(has_wiki)	Either true to enable the wiki for this repository or false to disable it
has_discussions(has_discussions)	True if the repository has discussions
Allow Forking(allow_forking)	True if the repository allows forking
Visibility(visibility)	The visibility of the repository (public or private)
Created at(created_at)	The timestamp when the update of the repository was initialised
Updated at(updated_at)	The timestamp when the update of the repository was updated
Pushed at(pushed_at)	The timestamp when the update of the repository was pushed

Github/Delete Repository method

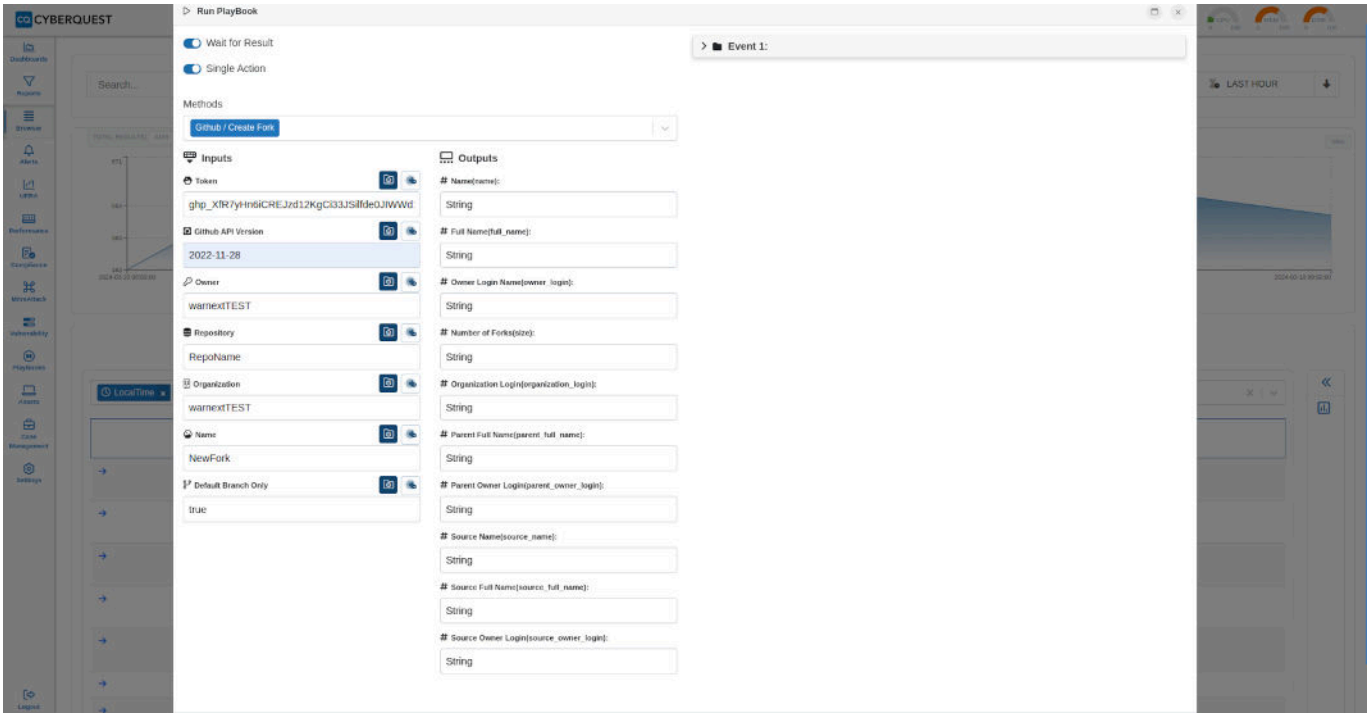
Delete the repository given by user.



Inputs	Description
Token (is required)	To use the Github API, you must have an API key
Github API Version (is required)	This parameter it is used to specify the version of the GitHub API being utilized
Owner (is required)	The account owner of the repository
Repository (is required)	The name of the repository without the .git extension

Github/Create Fork method

Create a fork for the authenticated user.

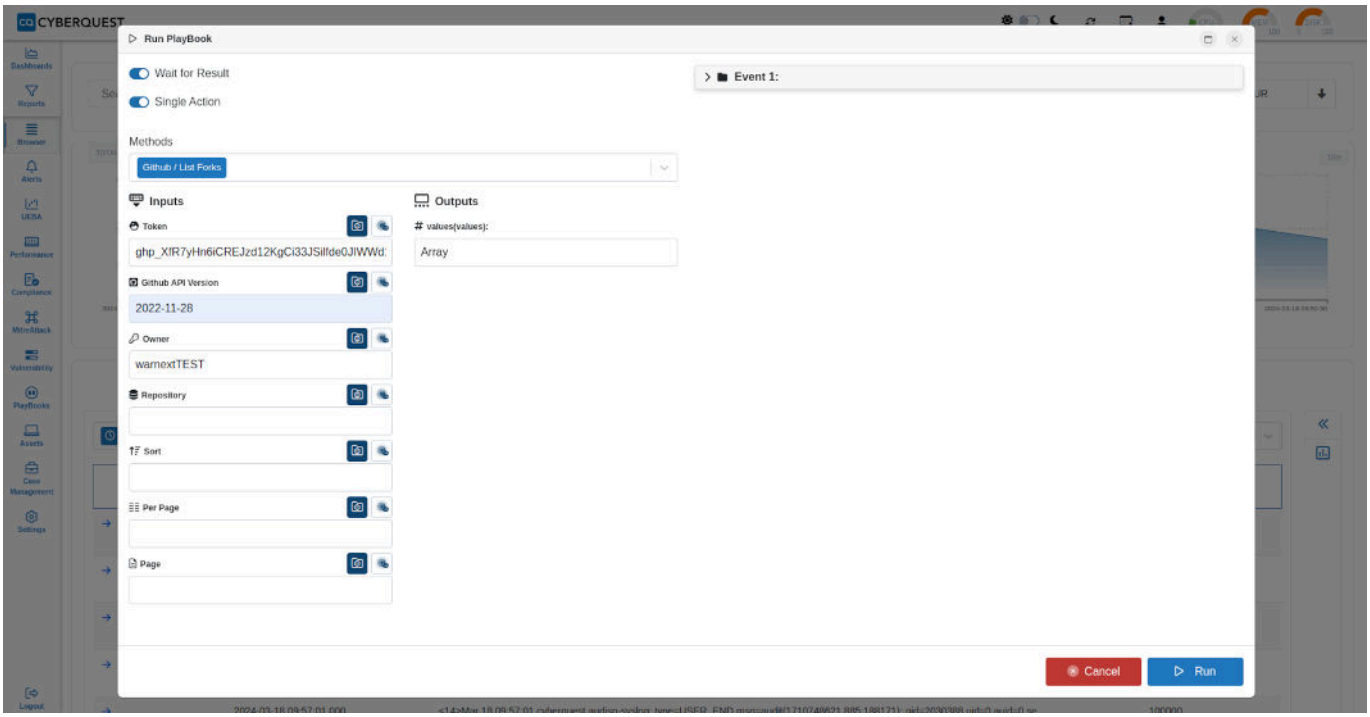


Inputs	Description
Token (is required)	To use the Github API, you must have an API key
Github API Version (is required)	This parameter it is used to specify the version of the GitHub API being utilized
Owner (is required)	The account owner of the repository
Repository (is required)	The name of the repository without the .git extension
Organization (is required)	Parameter to specify the organization name if forking into an organization
Name (is required)	When forking from an existing repository, a new name for the fork
Default Branch Only (is required)	When forking from an existing repository, fork with only the default branch

Outputs	Description
Name(name)	The name of the fork
Full Name(full_name)	The full name of the fork
Owner Login Name(owner_login)	The login name of the owner of the fork
Number of Forks(size)	The number of the forks created
Organization Login(organization_login)	The login name of the organization
Parent Full Name(parent_full_name)	The full name of the fork parent
Parent Owner Login(parent_owner_login)	The owner login name of the fork parent
Source Name(source_name)	The source name of the fork
Source Full Name(source_full_name)	The source full name of the fork
Source Owner Login(source_owner_login)	Source owner login name of the fork

Github/List Forks method

List Forks for a repository.

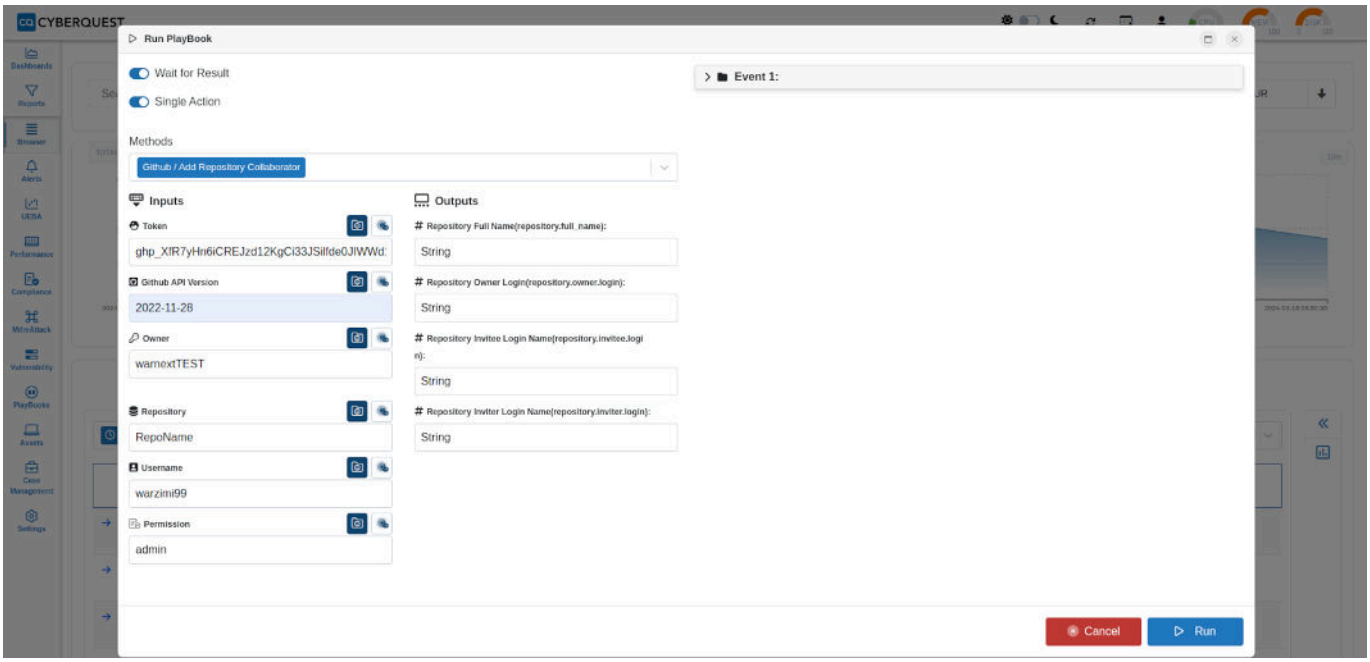


Inputs	Description
Token (is required)	To use the Github API, you must have an API key
Github API Version (is required)	This parameter it is used to specify the version of the GitHub API being utilized
Owner (is required)	The account owner of the repository
Repository (is required)	The name of the repository without the .git extension
Sort	The sort order. stargazers will sort by star count
Per Page	The number of results per page (max 100)
Page	Page number of the results to fetch

Outputs	Description
values(values)	The results of the API call

Github/Add Repository Collaborator method

Add a external colaborator to the repository.

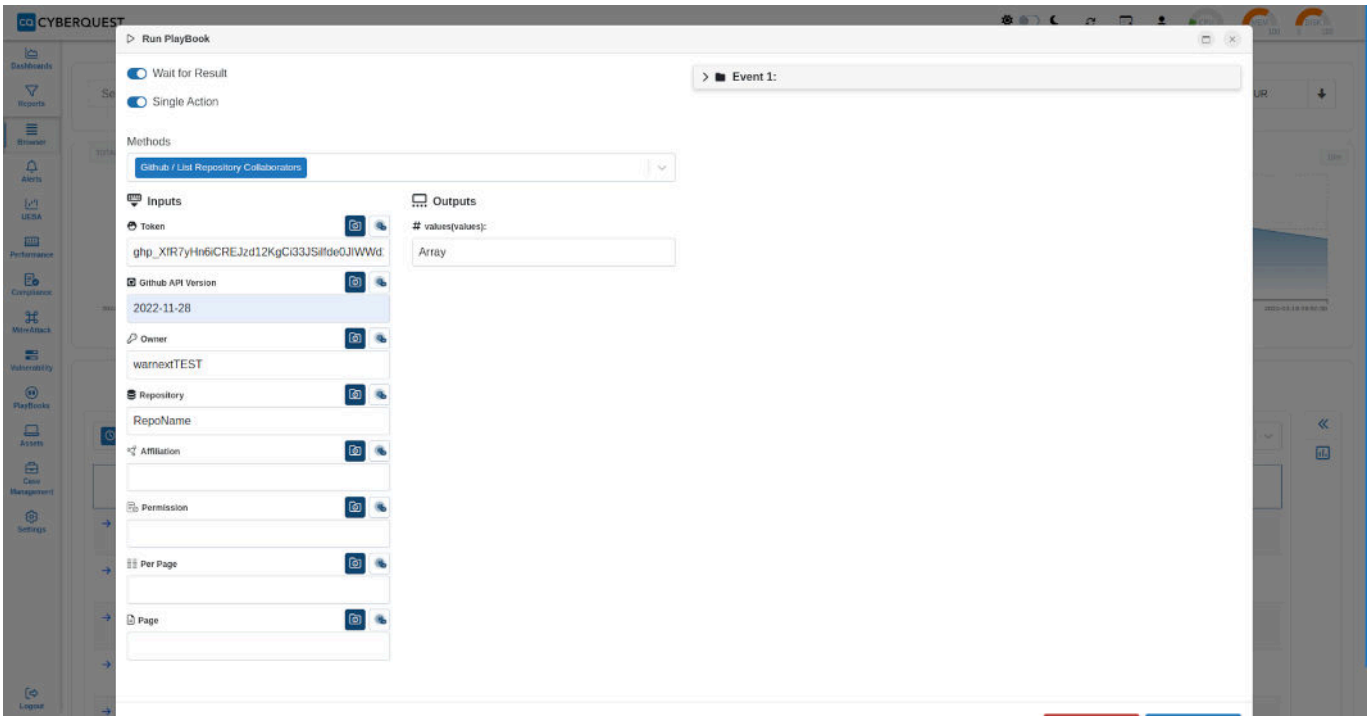


Inputs	Description
Token (is required)	To use the Github API, you must have an API key
Github API Version (is required)	This parameter it is used to specify the version of the GitHub API being utilized
Owner (is required)	The account owner of the repository
Repository (is required)	The name of the repository without the .git extension
Username (is required)	The handle for the GitHub user account.
Permission (is required)	The permission to grant the collaborator

Outputs	Description
Repository Full Name(repository.full_name)	The full name of the repository
Repository Owner Login(repository.owner.login)	The login name of the owner of the repository
Repository Invitee Login Name(repository.invitee.login)	The login name of the invitee
Repository Inviter Login Name(repository.inviter.login)	The login name of the inviter

Github/List Repository Collaborators method

This applies to organization-owned repositories. Collaborators encompass outside collaborators, direct/indirect organization members, and owners. Members with certain privileges can employ this endpoint.

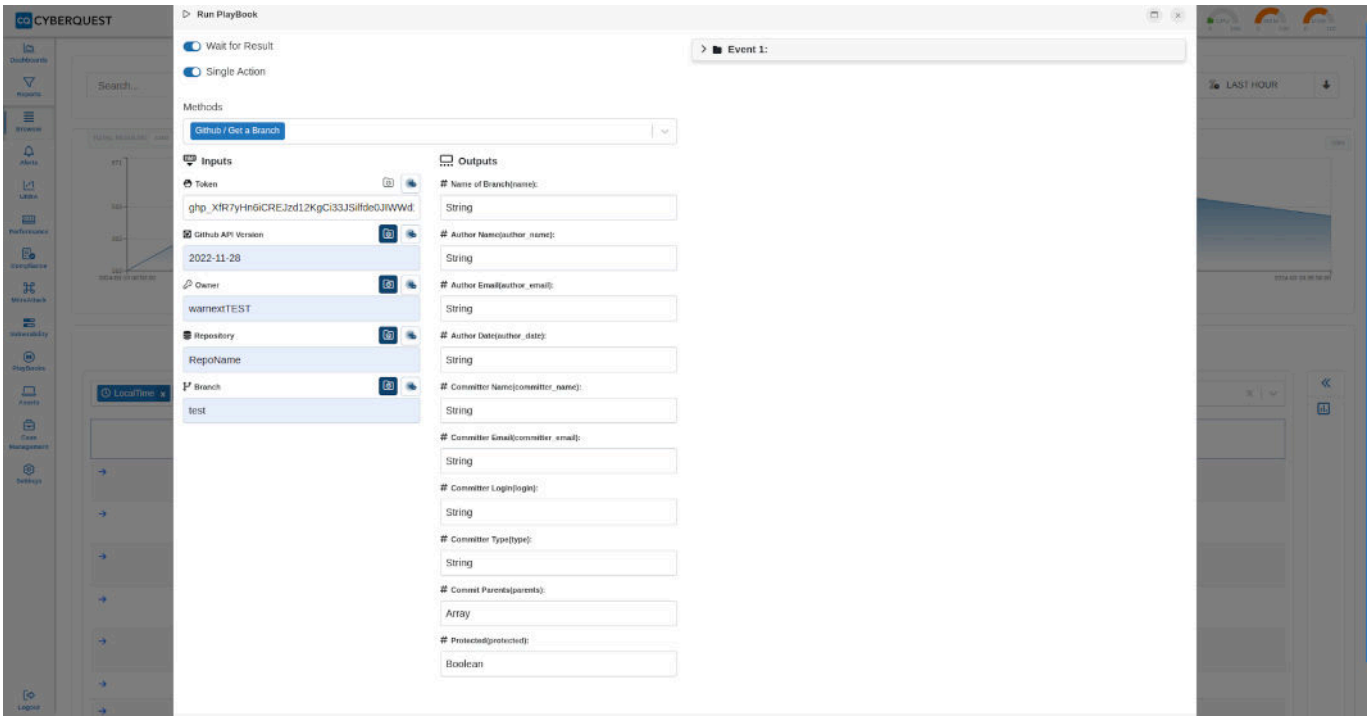


Inputs	Description
Token (is required)	To use the Github API, you must have an API key
Github API Version (is required)	This parameter it is used to specify the version of the GitHub API being utilized
Owner (is required)	The account owner of the repository
Repository (is required)	The name of the repository without the .git extension
Affiliation	Filter collaborators returned by their affiliation
Permission	Filter collaborators by the permissions they have on the repository. If not specified, all collaborators will be returned
Per Page	The number of results per page (max 100)
Page	Page number of the results to fetch

Outputs	Description
values(values)	The result of the API call

Github/Get a Branch method

Returns a branch selected by the user.

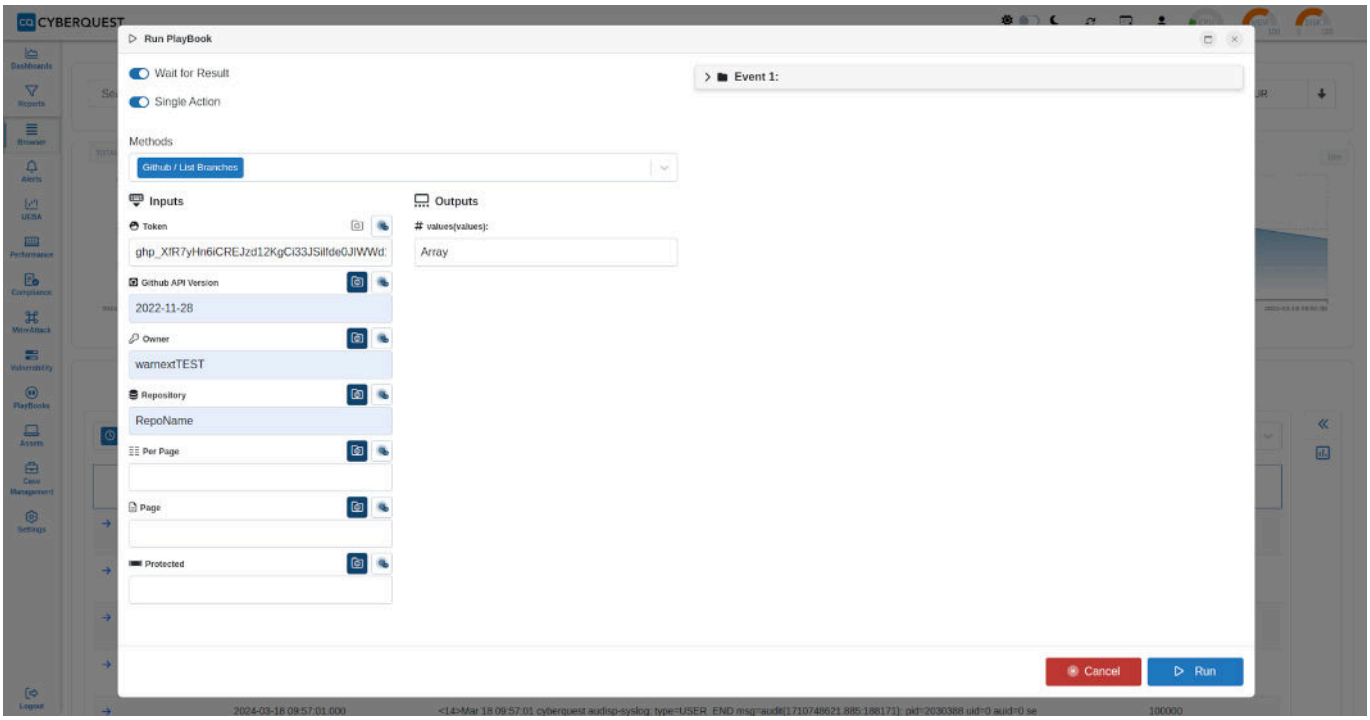


Inputs	Description
Token (is required)	To use the Github API, you must have an API key
Github API Version (is required)	This parameter it is used to specify the version of the GitHub API being utilized
Owner (is required)	The account owner of the repository
Repository (is required)	The name of the repository without the .git extension
Branch (is required)	Filter collaborators returned by their affiliation

Outputs	Description
Name of Branch(name)	The name of the branch
Author Name(author_name)	The author of the branch
Author Email(author_email)	The email of the author
Author Date(author_date)	The timestamp when the branch was created
Committer Name(committer_name)	The name of the commiter
Committer Email(committer_email)	The committer email
Committer Login(login)	The committer login name
Committer Type(type)	The committer type
Commit Parents(parents)	The parent of the branch
Protected(protected)	True if the branch is protected

Github/List Branches method

List branches for the selected repository and user.

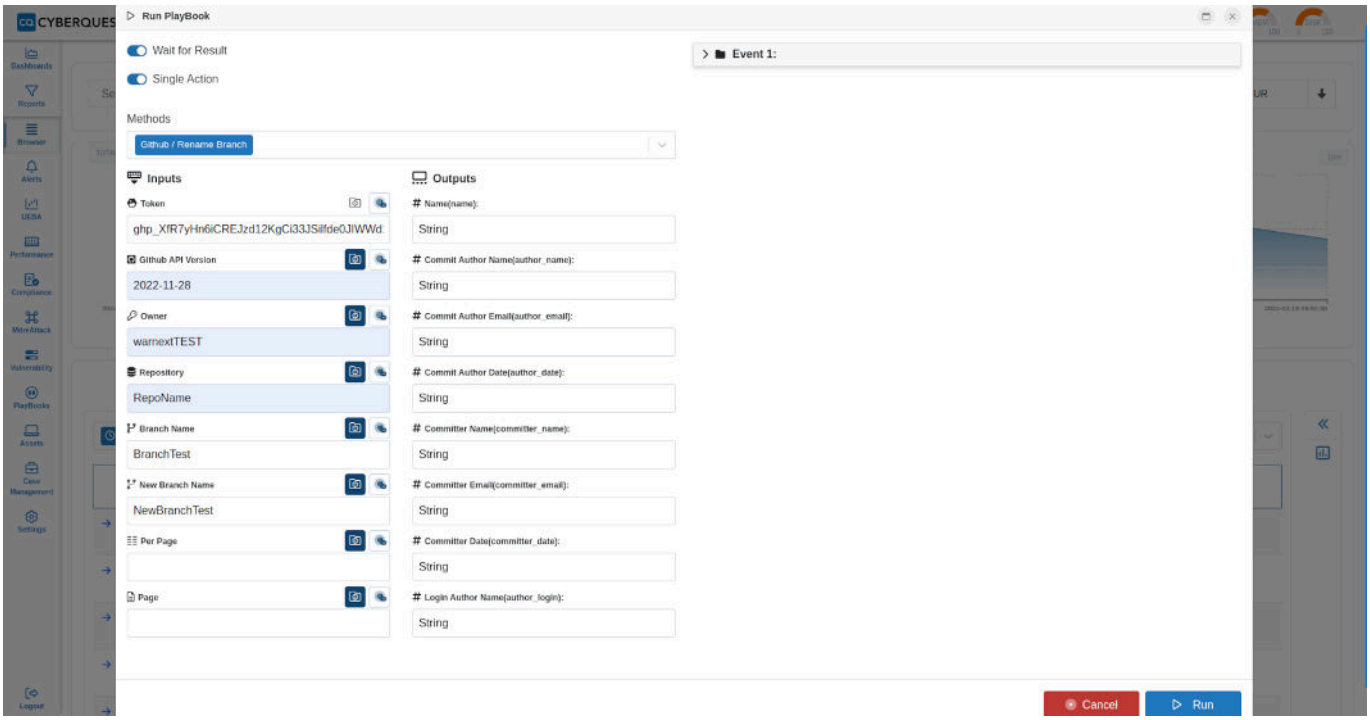


Inputs	Description
Token (is required)	To use the Github API, you must have an API key
Github API Version (is required)	This parameter it is used to specify the version of the GitHub API being utilized
Owner (is required)	The account owner of the repository
Repository (is required)	The name of the repository without the .git extension
Per Page	The number of results per page (max 100)
Page	Page number of the results to fetch
Protected	Setting to true returns only protected branches. When set to false, only unprotected branches are returned. Omitting this parameter returns all branches

Outputs	Description
values(values)	The result of the API call

Github/Rename Branch method

Rename a branch, selected by the user.

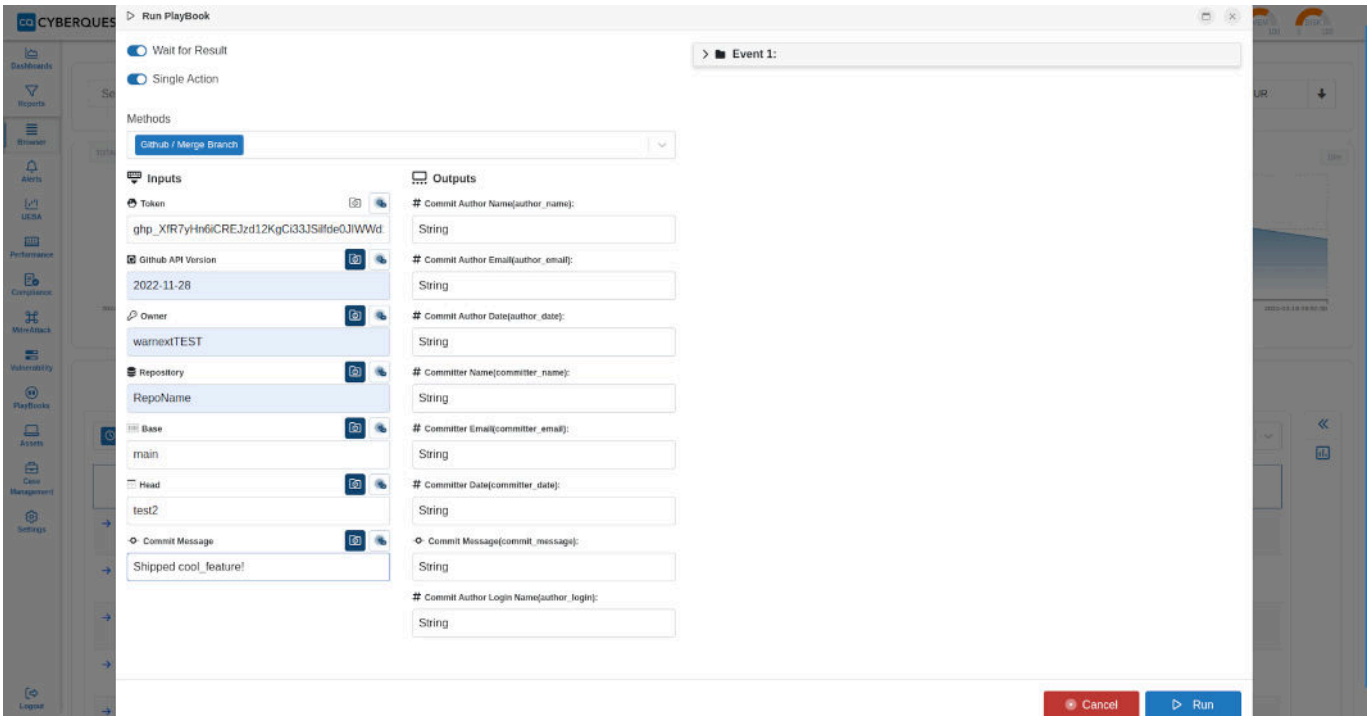


Inputs	Description
Token (is required)	To use the Github API, you must have an API key
Github API Version (is required)	This parameter it is used to specify the version of the GitHub API being utilized
Owner (is required)	The account owner of the repository
Repository (is required)	The name of the repository without the .git extension
Branch Name (is required)	The name of the repository without the .git extension
New Branch Name (is required)	The new name of the repository without the .git extension
Per Page	The number of results per page (max 100)
Page	Page number of the results to fetch

Outputs	Description
Name(name)	The new name of the branch
Commit Author Name(author_name)	The author name of the rename
Commit Author Email(author_email)	The author mail
Commit Author Date(author_date)	The timestamp when the author executed the operation
Committer Name(committer_name)	The name of the committer
Committer Email(committer_email)	The email of the committer
Committer Date(committer_date)	The timestamp when the commiter did actions
Login Author Name(author_login)	The name of login of author

Github/Merge Branch method

Merge selected branch.

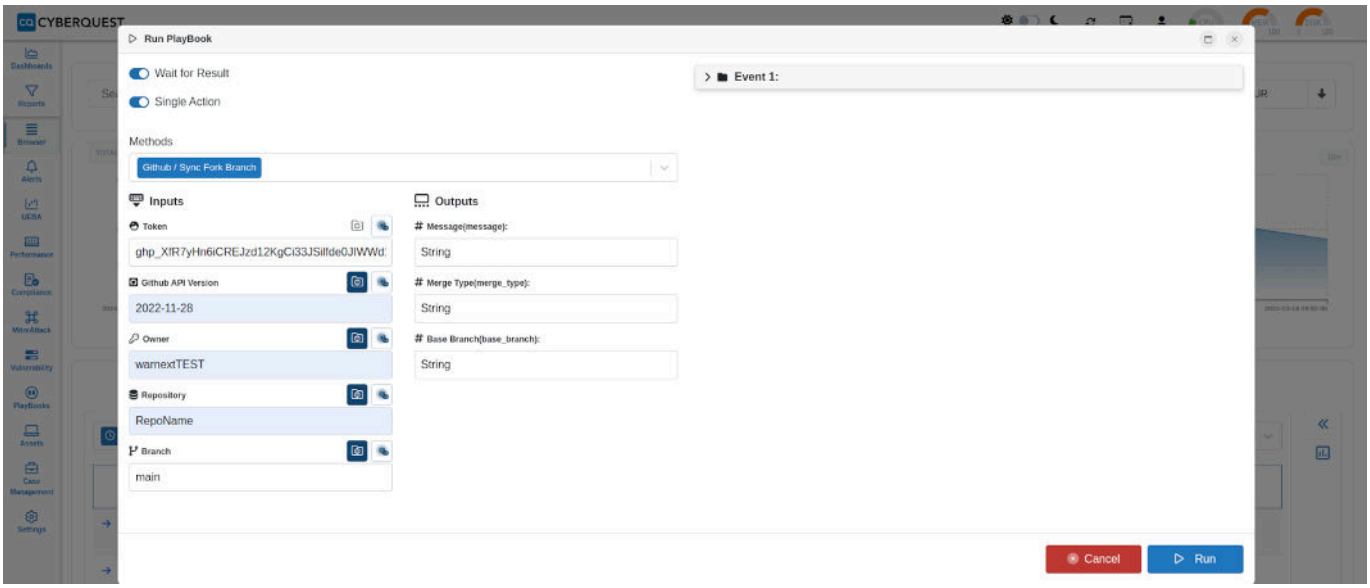


Inputs	Description
Token (is required)	To use the Github API, you must have an API key
Github API Version (is required)	This parameter it is used to specify the version of the GitHub API being utilized
Owner (is required)	The account owner of the repository
Repository (is required)	The name of the repository without the .git extension
Base (is required)	The name of the base branch that the head will be merged into
Head (is required)	The head to merge. This can be a branch name or a commit SHA1
Commit Message	Commit message to use for the merge commit. If omitted, a default message will be used

Outputs	Description
Commit Author Name(author_name)	The author name of the rename
Commit Author Email(author_email)	The author mail
Commit Author Date(author_date)	The timestamp when the author executed the operation
Committer Name(committer_name)	The name of the committer
Committer Email(committer_email)	The email of the committer
Committer Date(committer_date)	The timestamp when the commiter did actions
Commit Message(commit_message)	Commit message added by the user
Commit Author Login Name(author_login)	The name of login of author

Github/Sync Fork Branch method

Sync a branch of a forked repository to keep it up-to-date with the upstream repository.

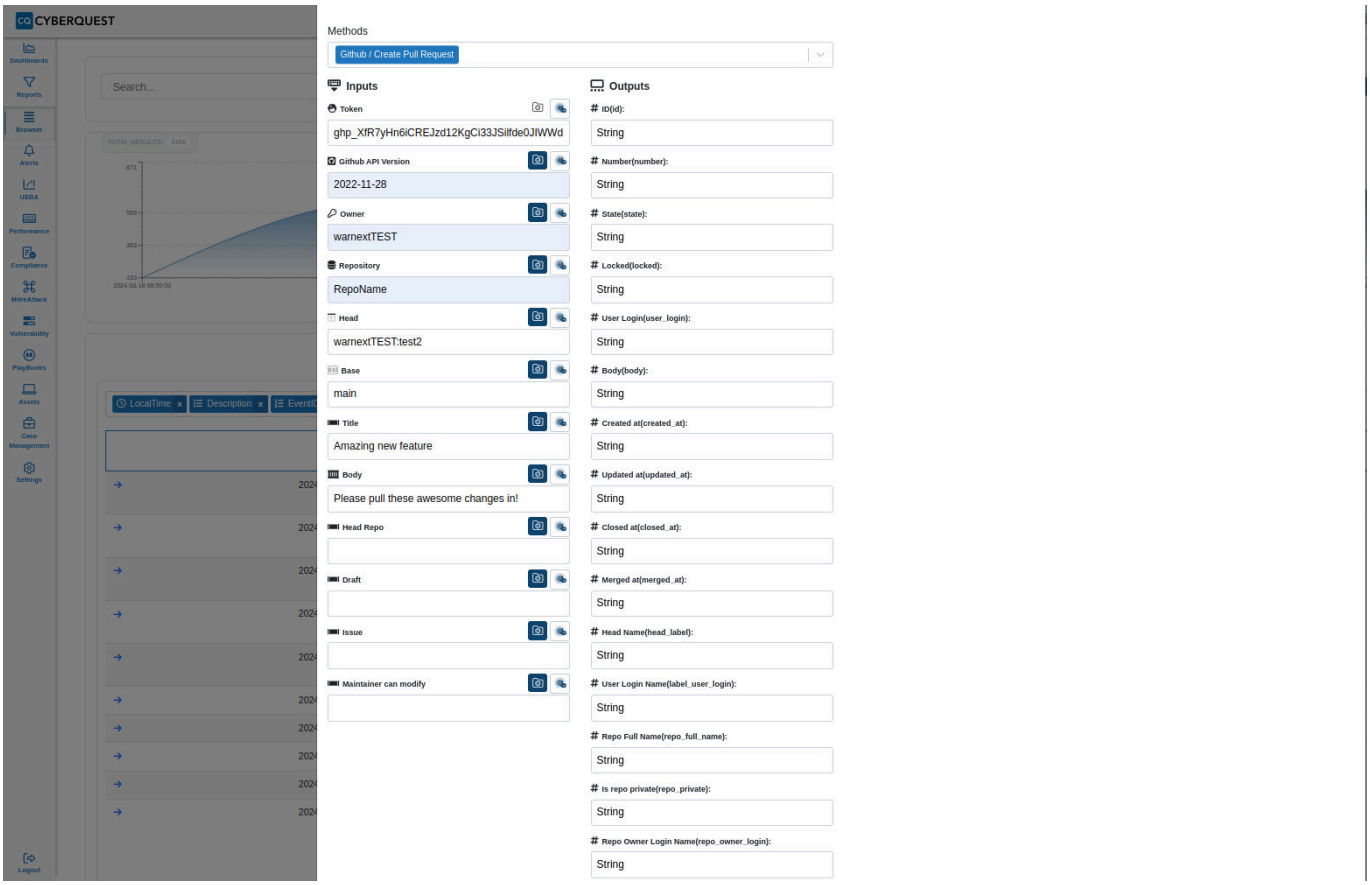


Inputs	Description
Token (is required)	To use the Github API, you must have an API key
Github API Version (is required)	This parameter it is used to specify the version of the GitHub API being utilized
Owner (is required)	The account owner of the repository
Repository (is required)	The name of the repository without the .git extension
Branch (is required)	The name of the branch which should be updated to match upstream

Outputs	Description
Message(message)	The message with details about sync process
Merge Type(merge_type)	The type of the merge
Base Branch(base_branch)	The name of the base branch

Github/Create Pull Request method

Creation of a Pull Request.

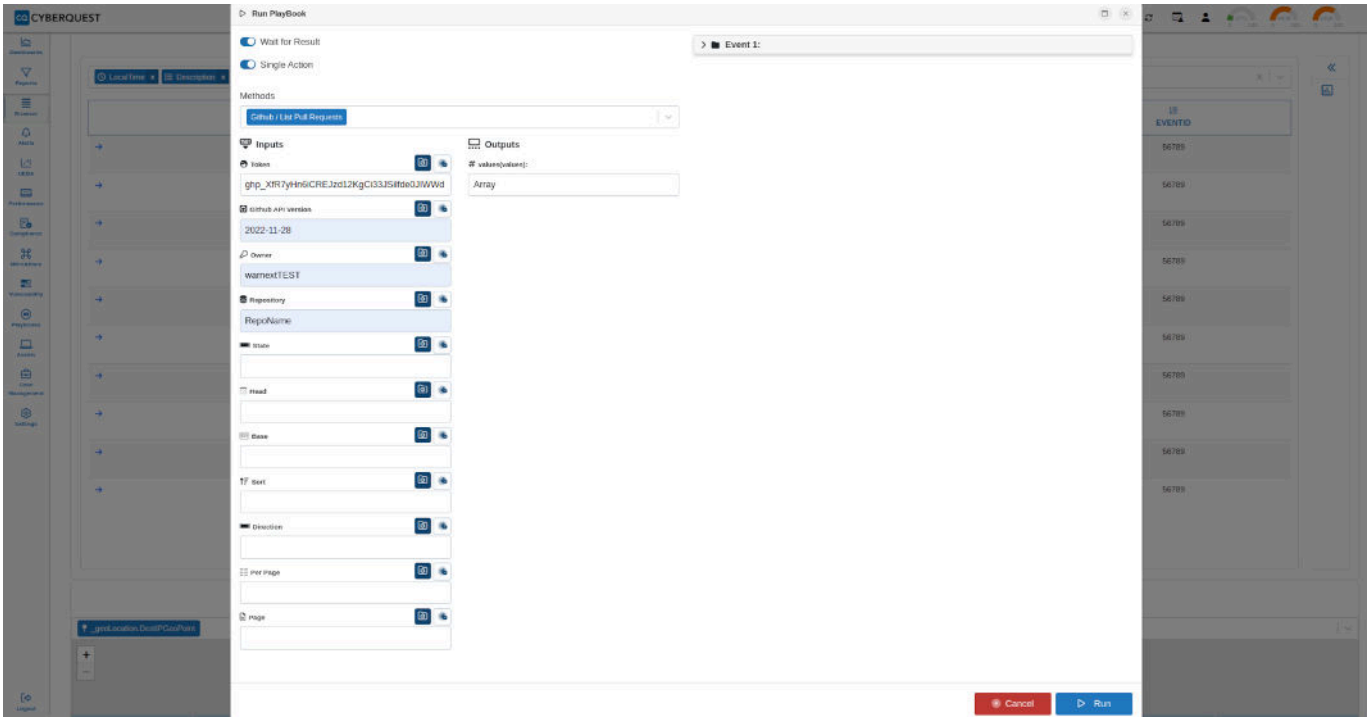


Inputs	Description
Token (is required)	To use the Github API, you must have an API key
Github API Version (is required)	This parameter it is used to specify the version of the GitHub API being utilized
Owner (is required)	The account owner of the repository
Repository (is required)	The name of the repository without the .git extension
Head (is required)	The name of the branch where your changes are implemented
Base (is required)	The name of the branch you want the changes pulled into. This should be an existing branch on the current repository. You cannot submit a pull request to one repository that requests a merge to a base of another repository
Title	The title of the new pull request. Required unless issue is specified
Body	The contents of the pull request
Head Repo	The name of the repository where the changes in the pull request were made. This field is required for cross-repository pull requests if both repositories are owned by the same organization.
Draft	Indicates whether the pull request is a draft
Issue	An issue in the repository to convert to a pull request. The issue title, body, and comments will become the title, body, and comments on the new pull request. Required unless title is specified
Maintainer can modify	Indicates whether maintainers can modify the pull request

Outputs	Description
ID(id)	The ID of the pull request
Number(number)	The number of the pull request
State(state)	The state of request
Locked(locked)	True if the pull requests are false, otherwise false
User Login(user_login)	The user login name
Body(body)	The content of the pull reuquest
Created at(created_at)	The timestamp when the pull request was created
Updated at(updated_at)	The timestamp when the pull request was updated
Closed at(closed_at)	The timestamp when the pull request was closed
Merged at(merged_at)	The timestamp when the merged was accomplished
Head Name(head_label)	The head name of the dead
User Login Name(label_user_login)	The user login name
Repo Full Name(repo_full_name)	The full name of the repository
Is repo private(repo_private)	True if the repository is private, otherwise is false
Repo Owner Login Name(repo_owner_login)	The login name of the repository owner

Github/List Pull Requests method

List all pull requests for the repo provided by the user.

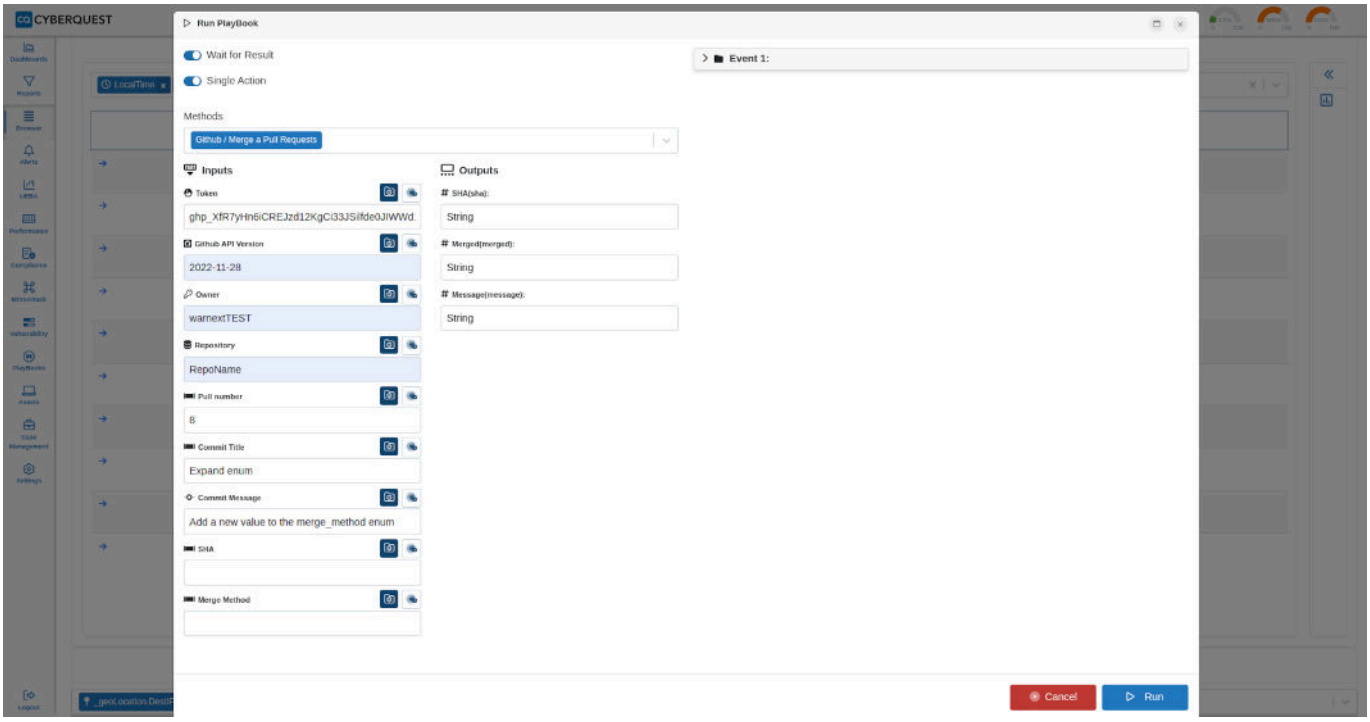


Inputs	Description
Token (is required)	To use the Github API, you must have an API key
Github API Version (is required)	This parameter it is used to specify the version of the GitHub API being utilized
Owner (is required)	The account owner of the repository
Repository (is required)	The name of the repository without the .git extension
State	Either open, closed, or all to filter by state
Head	Filter pulls by head user or head organization and branch name in the format of user:ref-name or organization:ref-name
Base	Filter pulls by base branch name
Sort	What to sort results by
Direction	The direction of the sort
Per Page	The number of results per page (max 100)
Page	Page number of the results to fetch

Outputs	Description
values(values)	The results of the API call

Github/Merge a Pull Requests method

Merges a pull request into the base branch.

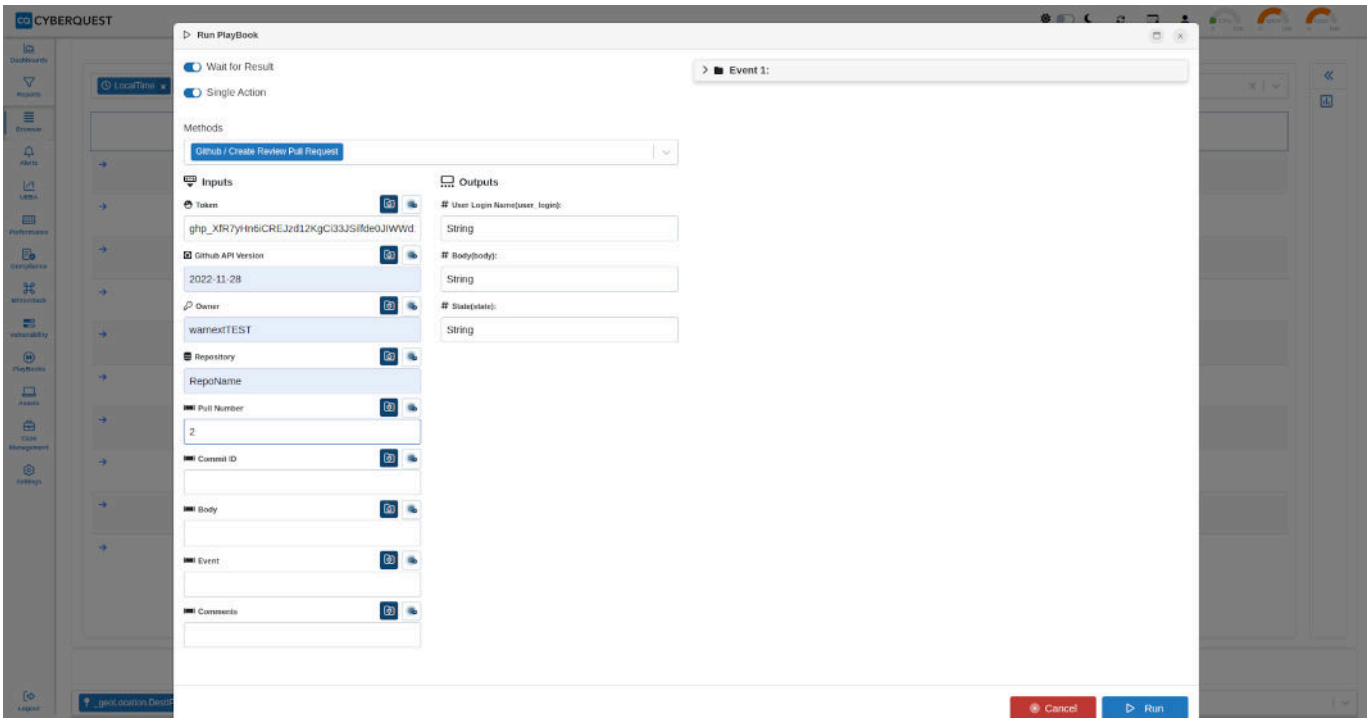


Inputs	Description
Token (is required)	To use the Github API, you must have an API key
Github API Version (is required)	This parameter it is used to specify the version of the GitHub API being utilized
Owner (is required)	The account owner of the repository
Repository (is required)	The name of the repository without the .git extension
Pull number (is required)	The number that identifies the pull request
Commit Title	Title for the automatic commit message
Commit Message	Extra detail to append to automatic commit message
SHA	SHA that pull request head must match to allow merge
Merge Method	The merge method to use

Outputs	Description
SHA(sha)	The SHA of the action
Merged(merged)	True if the merged was accomplished, otherwise false
Message(message)	The message with details about merge process

Github/Create Review Pull Request method

Create a review for a pull request.

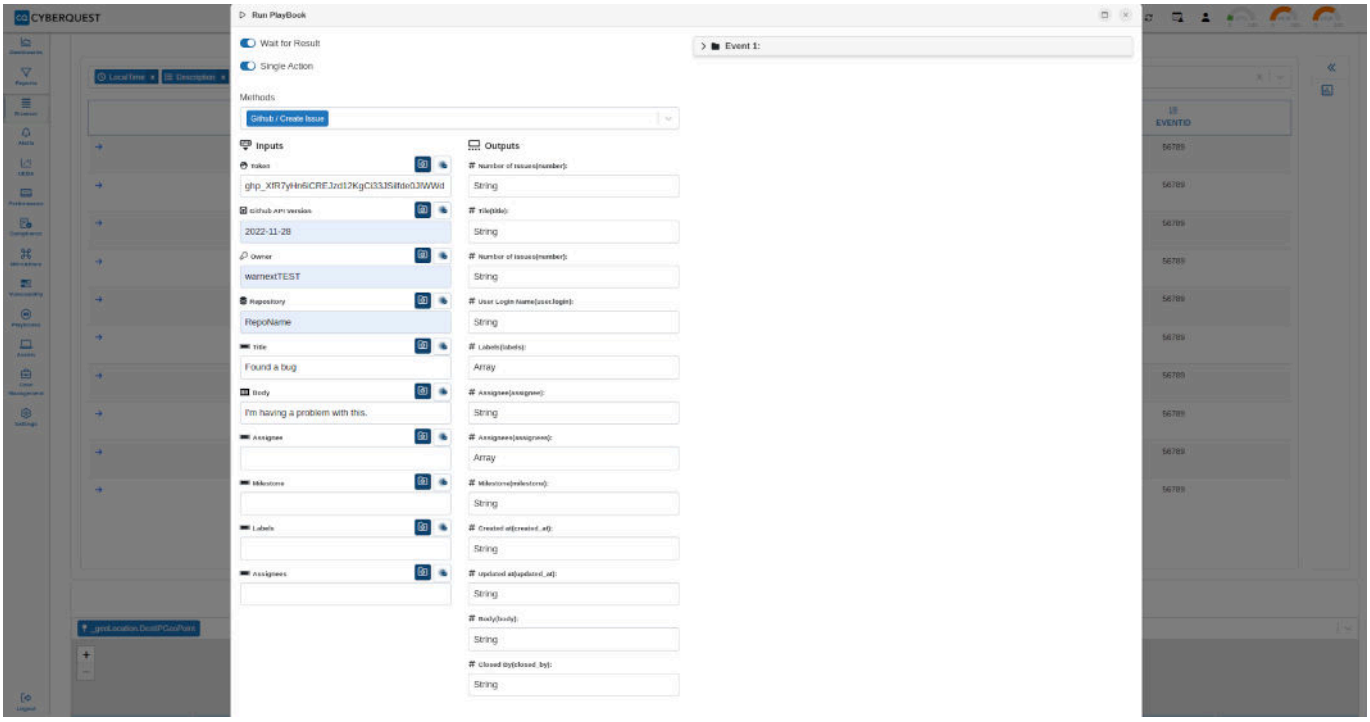


Inputs	Description
Token (is required)	To use the Github API, you must have an API key
Github API Version (is required)	This parameter it is used to specify the version of the GitHub API being utilized
Owner (is required)	The account owner of the repository
Repository (is required)	The name of the repository without the .git extension
Pull number (is required)	The number that identifies the pull request
Commit ID	The SHA of the commit needing a comment. Not using the latest commit SHA may render your comment outdated if a subsequent commit modifies the line you specify as the position
Body	The relative path to the file that necessitates a comment
Event	The number that identifies the pull request
Comments	The number that identifies the pull request

Outputs	Description
User Login Name(user_login)	The user login name
Body(body)	The description the release
State(state)	Either open, closed, or all to filter by state.

Github/Create Issue method

Any user with pull access to a repository can create an issue. If issues are disabled in the repository, the API returns a 410 Gone status.

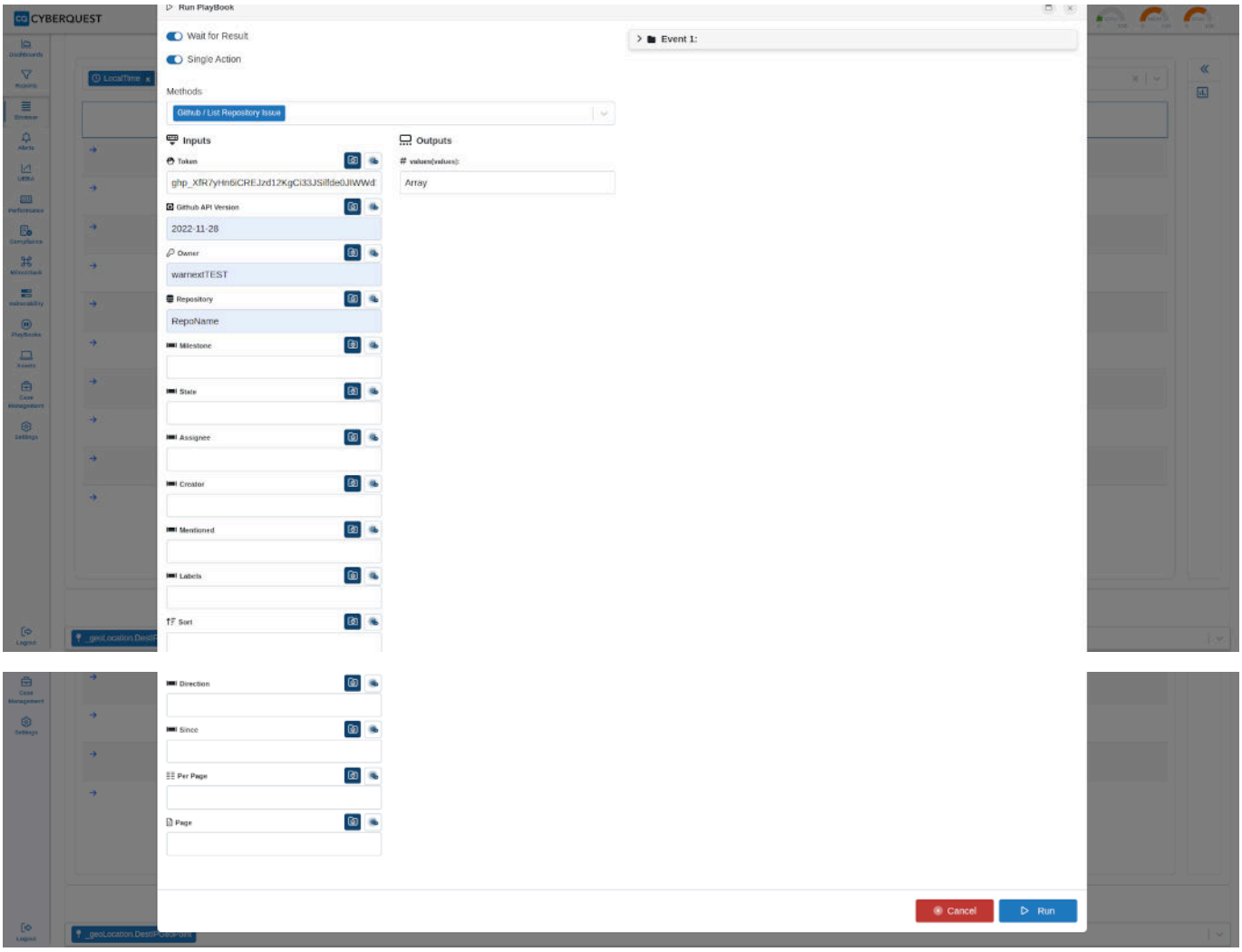


Inputs	Description
Token (is required)	To use the Github API, you must have an API key
Github API Version (is required)	This parameter it is used to specify the version of the GitHub API being utilized
Owner (is required)	The account owner of the repository
Repository (is required)	The name of the repository without the .git extension
Title (is required)	The title of the issue
Body (is required)	The contents of the issue
Assignee	Login for the user that this issue should be assigned to
Milestone	The number of the milestone to associate this issue with
Labels	Labels to associate with this issue
Assignees	Logins for Users to assign to this issue.

Outputs	Description
Number of Issues(number)	The number of the issues
Tile(title)	The title of the issues
User Login Name(user.login)	The login name of the user
Labels(labels)	Labels to associate with this issue. Pass one or more labels to replace the set of labels on this issue. Send an empty array ([]) to clear all labels from the issue. Only users with push access can set labels for issues. Without push access to the repository, label changes are silently dropped
Assignee(assignee)	Can be the name of a user. Pass in none for issues with no assigned user, and * for issues assigned to any user
Assignees(assignees)	Usernames to assign to this issue. Pass one or more user logins to replace the set of assignees on this issue. Send an empty array ([]) to clear all assignees from the issue. Only users with push access can set assignees for new issues. Without push access to the repository, assignee changes are silently dropped
Milestone(milestone)	The number of the milestone to associate this issue with or use null to remove the current milestone. Only users with push access can set the milestone for issues. Without push access to the repository, milestone changes are silently dropped
Created at(created_at)	The timestamp when the issue was created
Updated at(updated_at)	The timestamp when the issue was updated
Body(body)	The contents of the issue
Closed By(closed_by)	The name of the person who resolved/closed the issue

Github/List Repository Issue method

List issues in a repository. Only open issues will be listed.

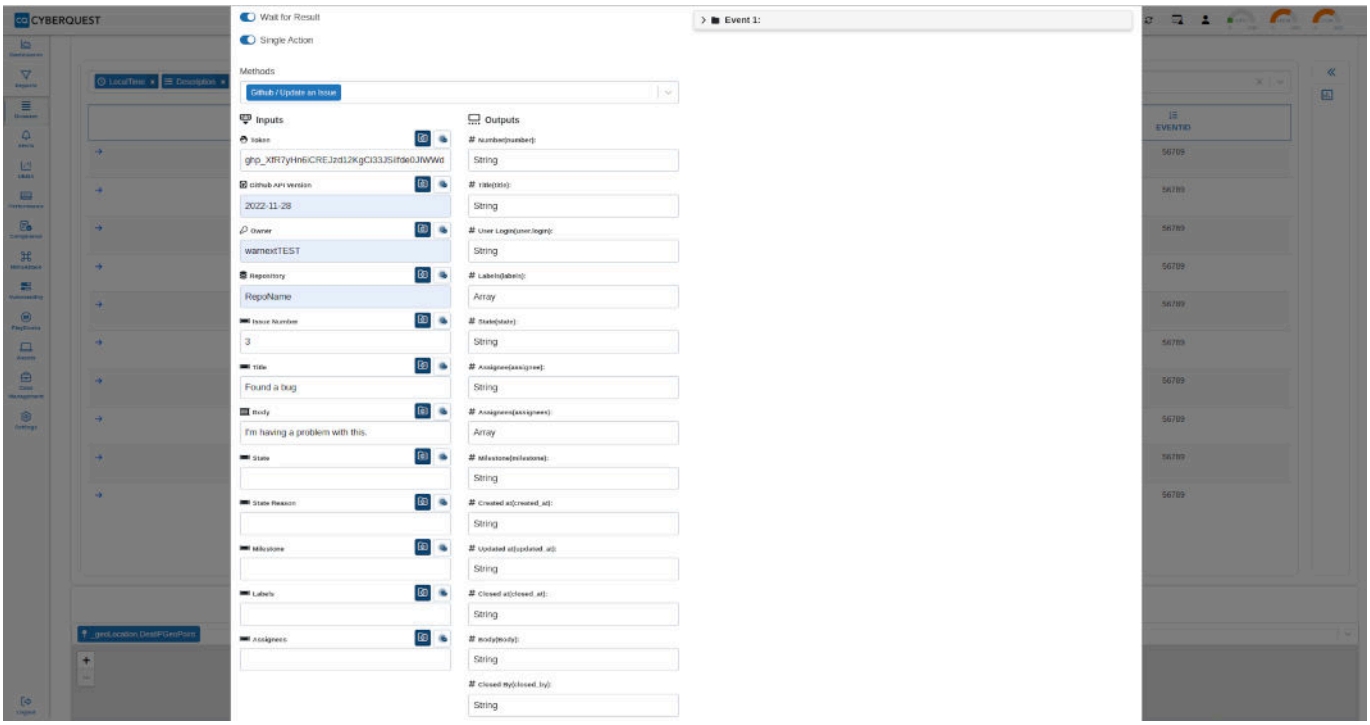


Inputs	Description
Token (is required)	To use the Github API, you must have an API key
Github API Version (is required)	This parameter it is used to specify the version of the GitHub API being utilized
Owner (is required)	The account owner of the repository
Repository (is required)	The name of the repository without the .git extension
Milestone	If an integer is passed, it should refer to a milestone by its number field. If the string * is passed, issues with any milestone are accepted. If the string none is passed, issues without milestones are returned
State	Indicates the state of the issues to return
Assignee	Can be the name of a user. Pass in none for issues with no assigned user, and * for issues assigned to any user
Creator	The user that created the issue
Mentioned	A user thats mentioned in the issue
Labels	A list of comma separated label names
Sort	What to sort results by
Direction	The direction to sort the results by
Since	Only show results that were last updated after the given time
Per Page	The number of results per page
Page	Page number of the results to fetch

Outputs	Description
values(values)	The result of the API call

Github/Update an Issue method

Issue owners and users with push access can edit an issue.

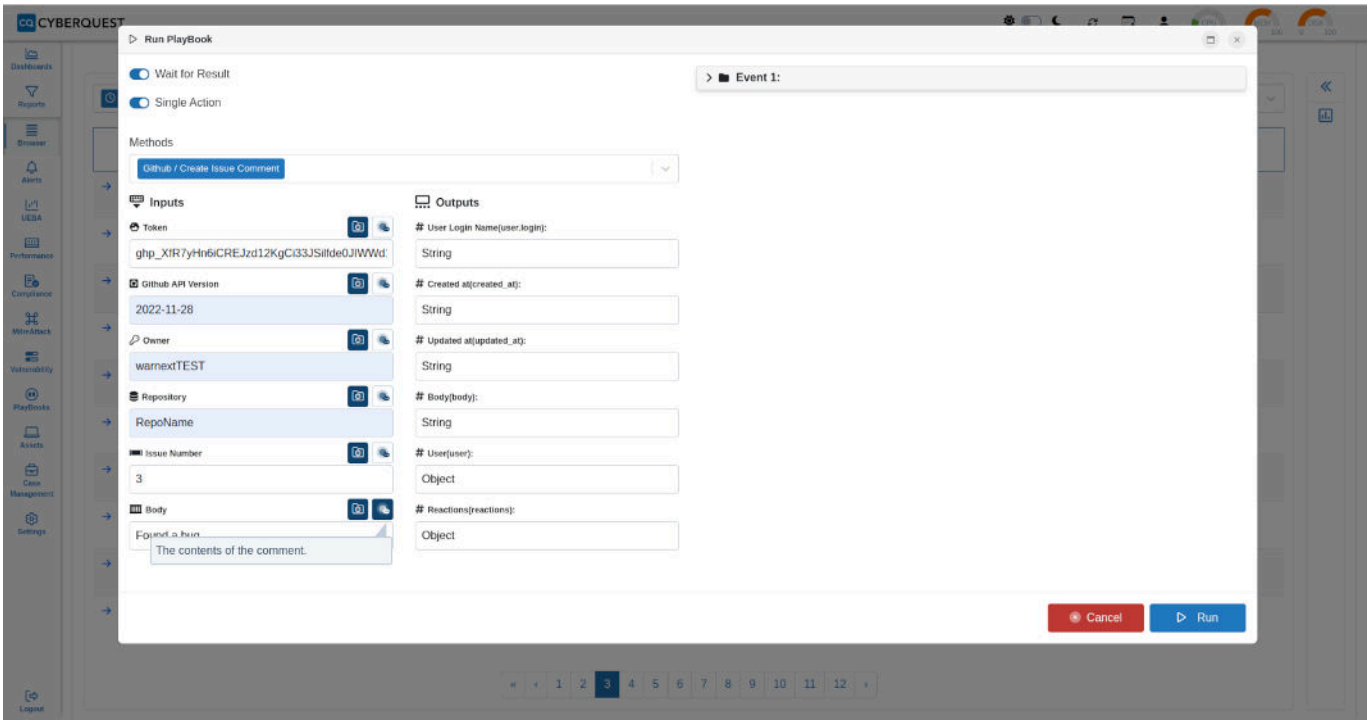


Inputs	Description
Token (is required)	To use the Github API, you must have an API key
Github API Version (is required)	This parameter it is used to specify the version of the GitHub API being utilized
Owner (is required)	The account owner of the repository
Repository (is required)	The name of the repository without the .git extension
Issue Number (is required)	The number that identifies the issue.
Title	The title of the issue
Body	The contents of the issue
State	The open or closed state of the issue
State Reason	The reason for the state change. Ignored unless state is changed
Milestone	The number of the milestone to associate this issue with or use null to remove the current milestone. Only users with push access can set the milestone for issues. Without push access to the repository, milestone changes are silently dropped
Labels	Labels to associate with this issue. Pass one or more labels to replace the set of labels on this issue. Send an empty array ([]) to clear all labels from the issue. Only users with push access can set labels for issues. Without push access to the repository, label changes are silently dropped
Assignees	Usernames to assign to this issue. Pass one or more user logins to replace the set of assignees on this issue. Send an empty array ([]) to clear all assignees from the issue. Only users with push access can set assignees for new issues. Without push access to the repository, assignee changes are silently dropped

Outputs	Description
Number(number)	The number of the issues
Title(title)	The title of the issue
User Login(user.login)	The login name of the user
Labels(labels)	Labels to associate with this issue. Pass one or more labels to replace the set of labels on this issue. Send an empty array ([]) to clear all labels from the issue. Only users with push access can set labels for issues. Without push access to the repository, label changes are silently dropped
State(state)	The open or closed state of the issue
Assignee(assignee)	Can be the name of a user. Pass in none for issues with no assigned user, and * for issues assigned to any user
Assignees(assignees)	Usernames to assign to this issue. Pass one or more user logins to replace the set of assignees on this issue. Send an empty array ([]) to clear all assignees from the issue. Only users with push access can set assignees for new issues. Without push access to the repository, assignee changes are silently dropped
Milestone(milestone)	The number of the milestone to associate this issue with or use null to remove the current milestone. Only users with push access can set the milestone for issues. Without push access to the repository, milestone changes are silently dropped
Created at(created_at)	The timestamp when the issue was created
Updated at(updated_at)	The timestamp when the issue was updated
Closed at(closed_at)	The timestamp when repository was created
Body(Body)	The contents of the issue
Closed By(closed_by)	The name of the person who resolved/closed the issue

Github/Create Issue Comment method

You can use the REST API to create comments on issues and pull requests. Every pull request is an issue, but not every issue is a pull request.

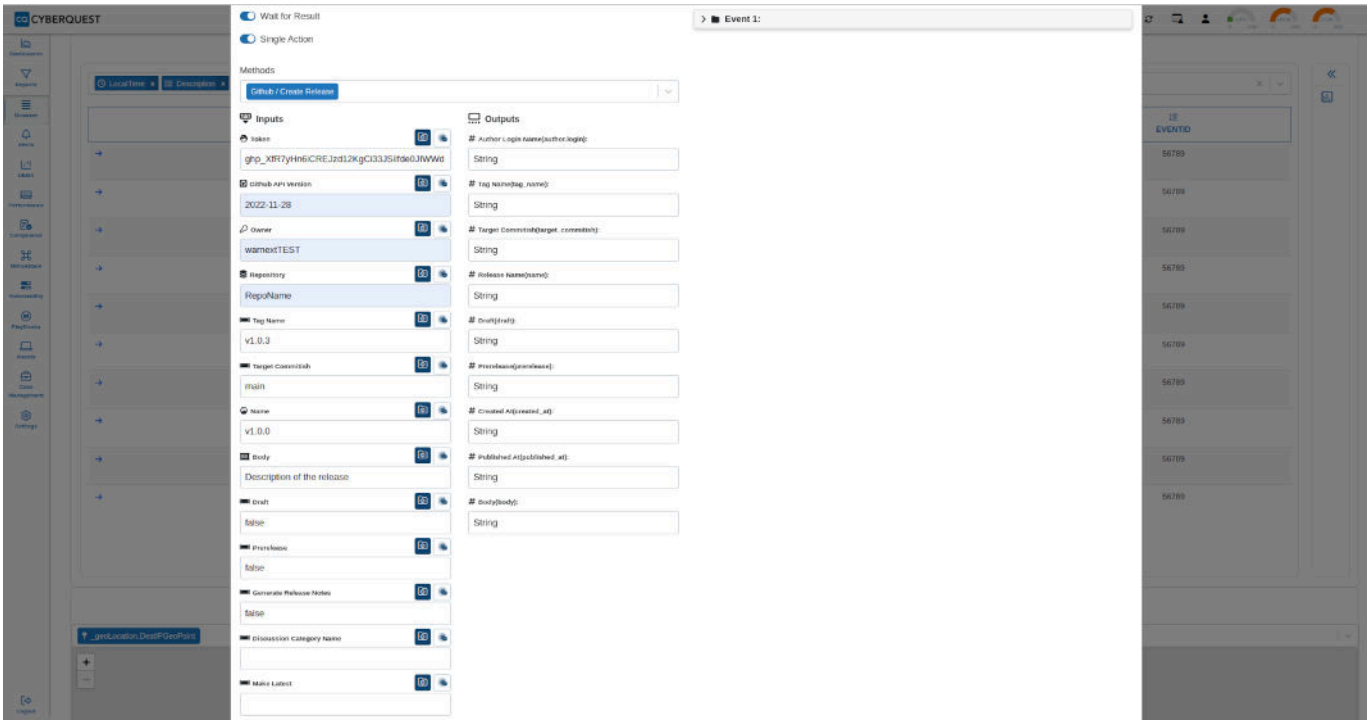


Inputs	Description
Token (is required)	To use the Github API, you must have an API key
Github API Version (is required)	This parameter it is used to specify the version of the GitHub API being utilized
Owner (is required)	The account owner of the repository
Repository (is required)	The name of the repository without the .git extension
Issue Number (is required)	The number that identifies the issue.
Body (is required)	The contents of the comment

Outputs	Description
User Login Name(user.login)	The login name of the user
Created at(created_at)	The timestamp when the issue comment was created
Updated at(updated_at)	The timestamp when the issue comment was updated
Body(Body)	The contents of the issue comment
User(user)	User details
Reactions(reactions)	A list with reactions of different users for the comment

Github/Create Release method

Users with push access to the repository can create a release.

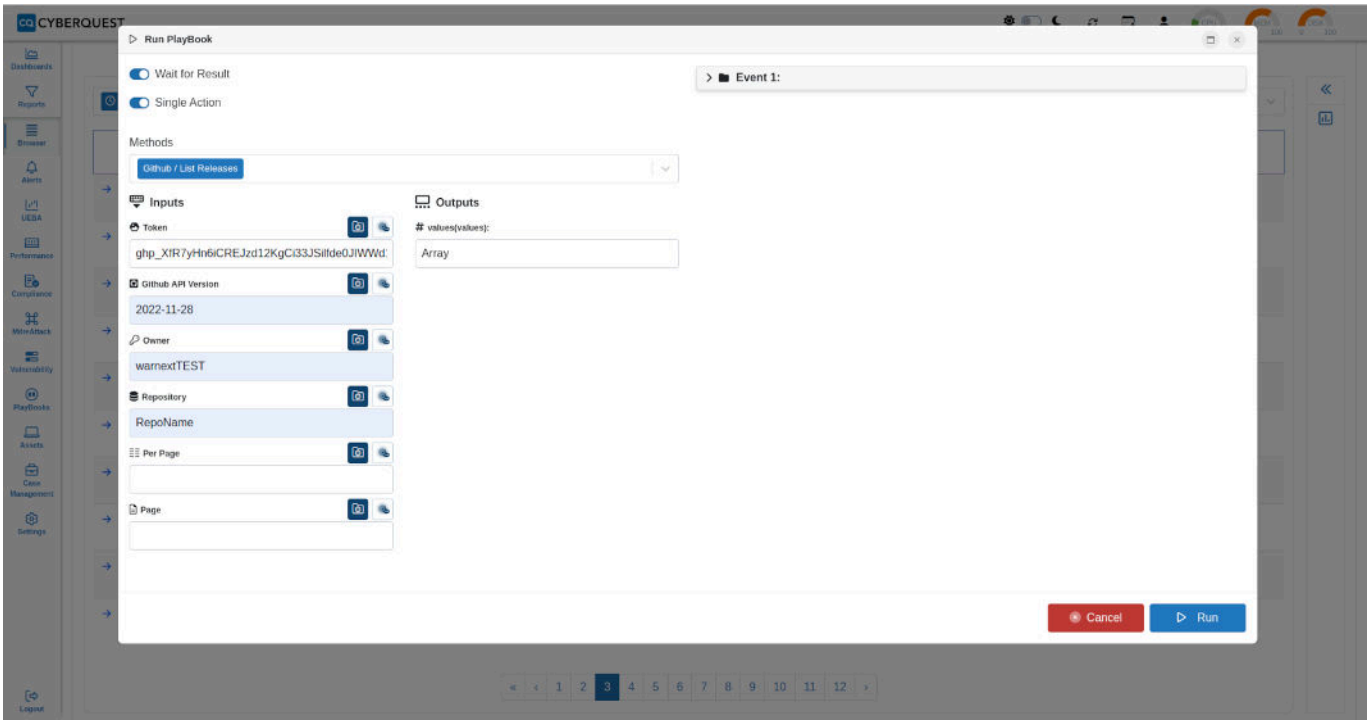


Inputs	Description
Token (is required)	To use the Github API, you must have an API key
Github API Version (is required)	This parameter it is used to specify the version of the GitHub API being utilized
Owner (is required)	The account owner of the repository
Repository (is required)	The name of the repository without the .git extension
Tag Name (is required)	The name of the tag
Target Commitish	Specifies the commitish value that determines where the Git tag is created from. Can be any branch or commit SHA. Unused if the Git tag already exists. Default: the repositorys default branch
Name	The name of the release
Body	The name of the tag
Draft	True to create a draft (unpublished) release, false to create a published one.
Prerelease	True to identify the release as a prerelease. false to identify the release as a full release.
Generate Release Notes	Whether to automatically generate the name and body for this release. If name is specified, the specified name will be used; otherwise, a name will be automatically generated. If body is specified, the body will be pre-pended to the automatically generated notes
Discussion Category Name	If specified, a discussion of the specified category is created and linked to the release. The value must be a category that already exists in the repository
Make Latest	Specifies whether this release should be set as the latest release for the repository

Outputs	Description
Author Login Name(author.login)	The login name of the author
Tag Name(tag_name)	The version of the release
Target Commitish(target_commitish)	The name of the branch which is used for release
Release Name(name)	The name of the release
Draft(draft)	True if the release is draft, otherwise false
Prerelease(prerelease)	True if it is prerelease, otherwise false
Created At(created_at)	The timestamp when the release was created
Published At(published_at)	The timestamp when the release was published
Body(body)	The description the release

Github/List Releases method

This returns a list of releases, which does not include regular Git tags that have not been associated with a release.

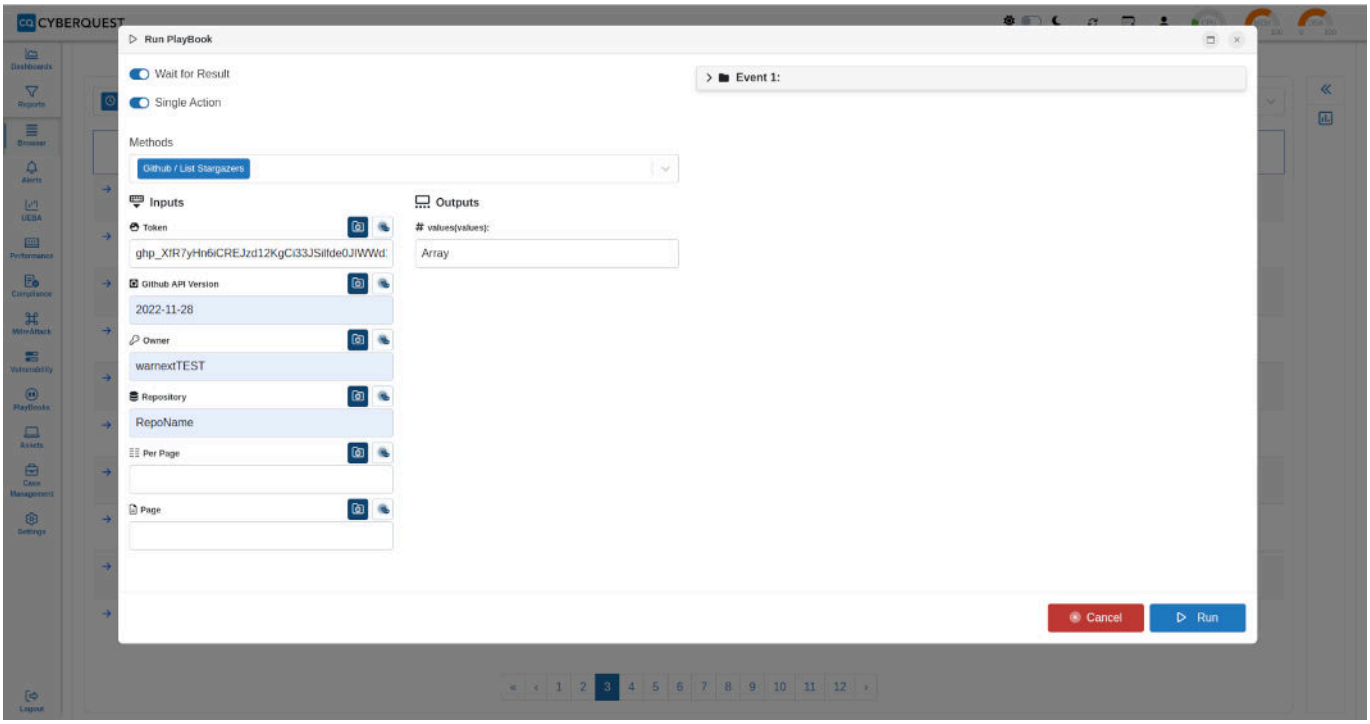


Inputs	Description
Token (is required)	To use the Github API, you must have an API key
Github API Version (is required)	This parameter it is used to specify the version of the GitHub API being utilized
Owner (is required)	The account owner of the repository
Repository (is required)	The name of the repository without the .git extension
Per Page	The number of results per page (max 100)
Page	Page number of the results to fetch

Outputs	Description
values(values)	The results of the API call

Github/List Stargazers method

Lists the people that have starred the repository.

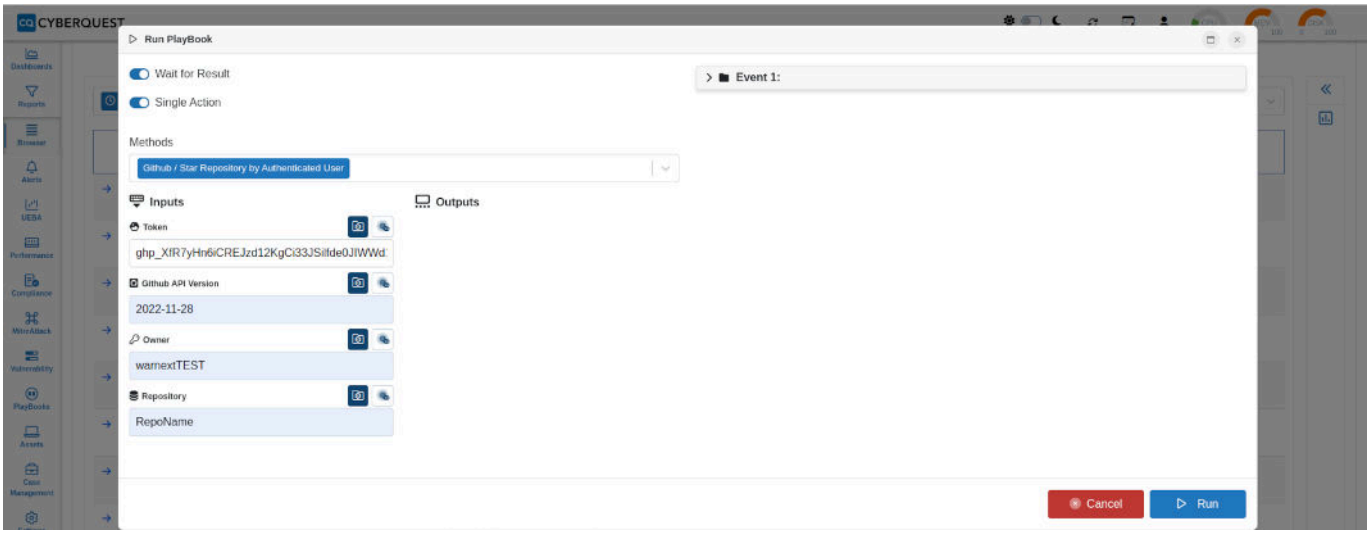


Inputs	Description
Token (is required)	To use the Github API, you must have an API key
Github API Version (is required)	This parameter it is used to specify the version of the GitHub API being utilized
Owner (is required)	The account owner of the repository
Repository (is required)	The name of the repository without the .git extension
Per Page	The number of results per page (max 100)
Page	Page number of the results to fetch

Outputs	Description
values(values)	The result of the API call

Github/Star Repository by Authenticated User method

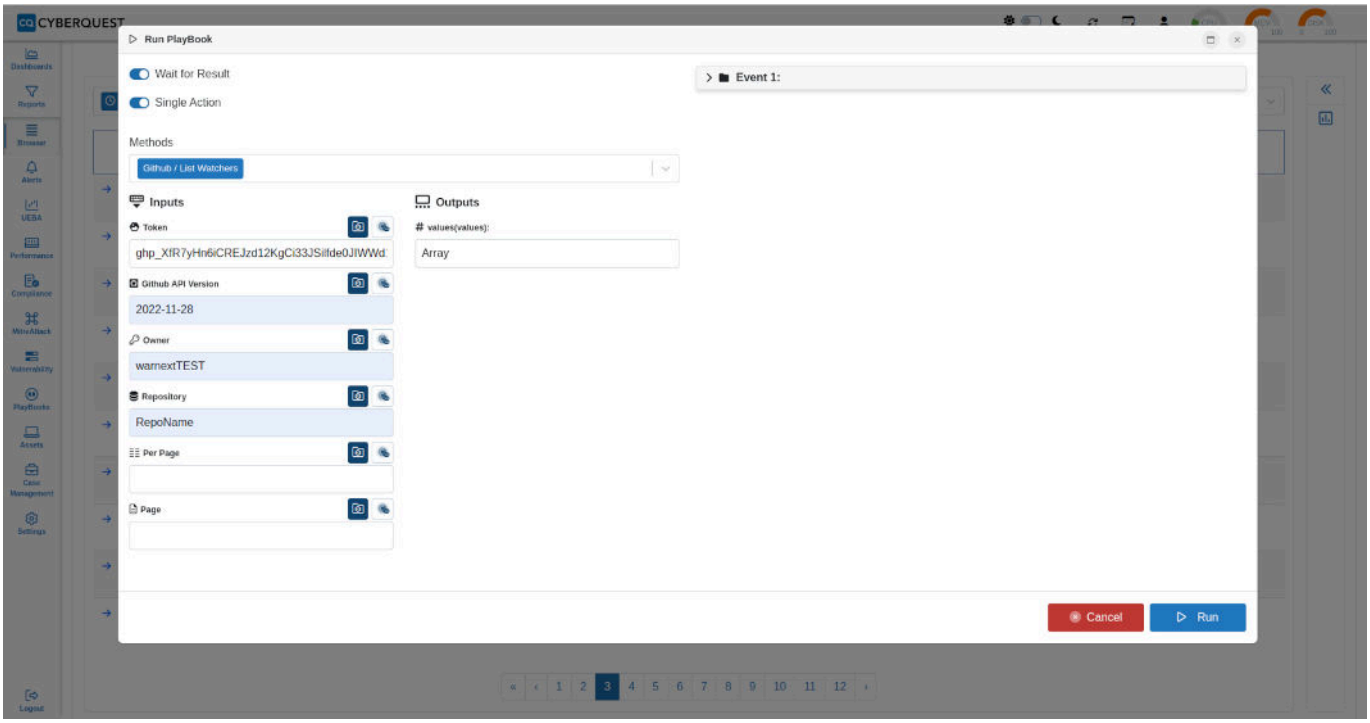
Lists repositories the authenticated user has starred.



Inputs	Description
Token (is required)	To use the Github API, you must have an API key
Github API Version (is required)	This parameter it is used to specify the version of the GitHub API being utilized
Owner (is required)	The account owner of the repository
Repository (is required)	The name of the repository without the .git extension

Github/List Watchers method

Lists the people watching the specified repository.

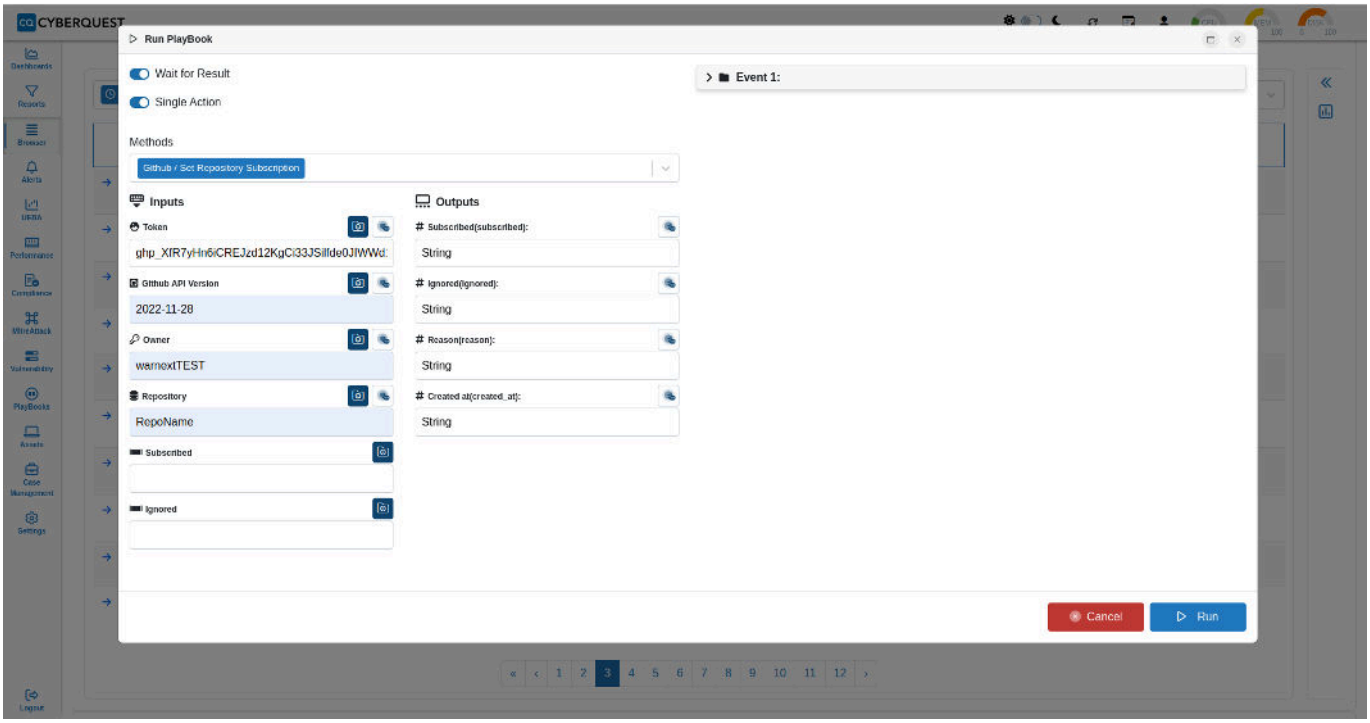


Inputs	Description
Token (is required)	To use the Github API, you must have an API key
Github API Version (is required)	This parameter it is used to specify the version of the GitHub API being utilized
Owner (is required)	The account owner of the repository
Repository (is required)	The name of the repository without the .git extension
Per Page	The number of results per page (max 100)
Page	Page number of the results to fetch

Outputs	Description
values(values)	The result of the API call

Github/Set Repository Subscription method

If you would like to watch a repository, set subscribed to true.



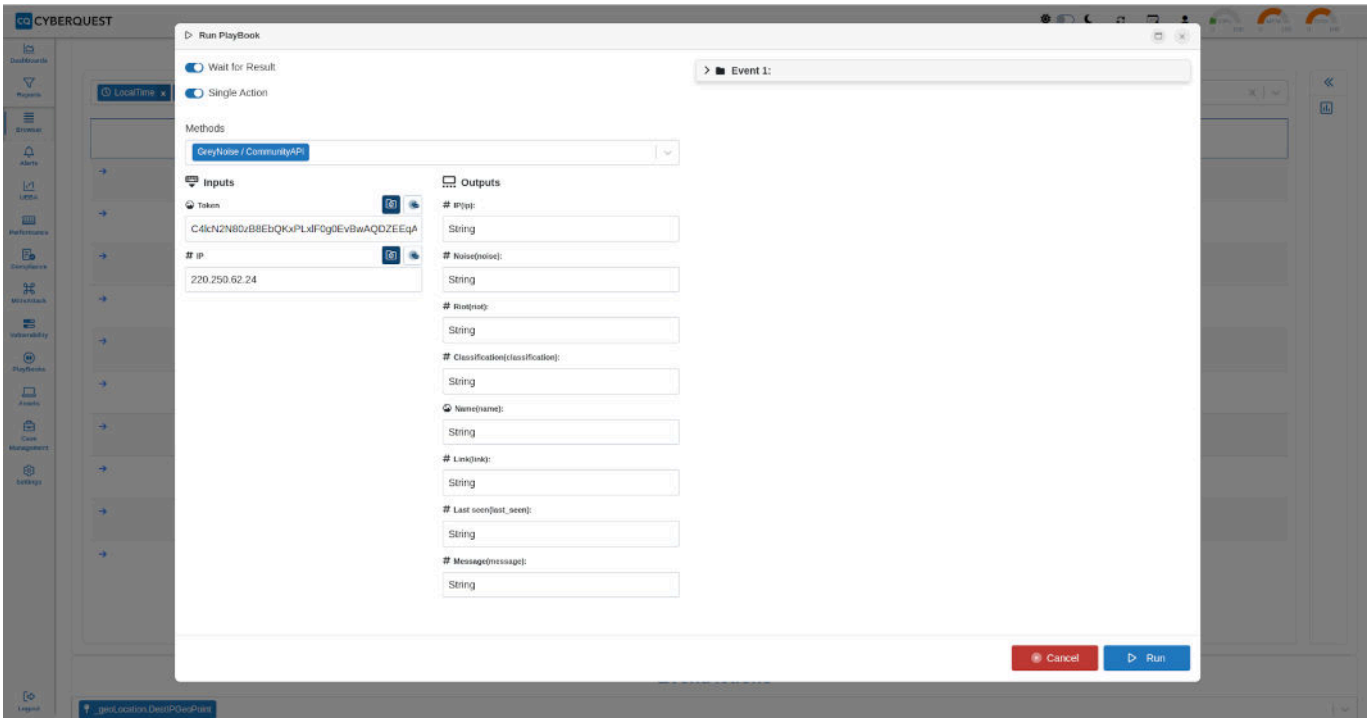
Inputs	Description
Token (is required)	To use the Github API, you must have an API key
Github API Version (is required)	This parameter it is used to specify the version of the GitHub API being utilized
Owner (is required)	The account owner of the repository
Repository (is required)	The name of the repository without the .git extension
Subscribed (is required)	The number of results per page (max 100)
Ignored (is required)	Page number of the results to fetch

Outputs	Description
Subscribed(subscribed)	Determines if notifications should be received from this repository
Ignored(ignored)	Determines if all notifications should be blocked from this repository
Reason(reason)	Description about why the action was taken
Created at(created_at)	The timestamp when you subscribed to a repository

GreyNoise

GreyNoise/CommunityAPI method

The Community API provides community users with a free tool to query IPs in the GreyNoise dataset and retrieve a subset of the full IP context data returned by the IP Lookup API.



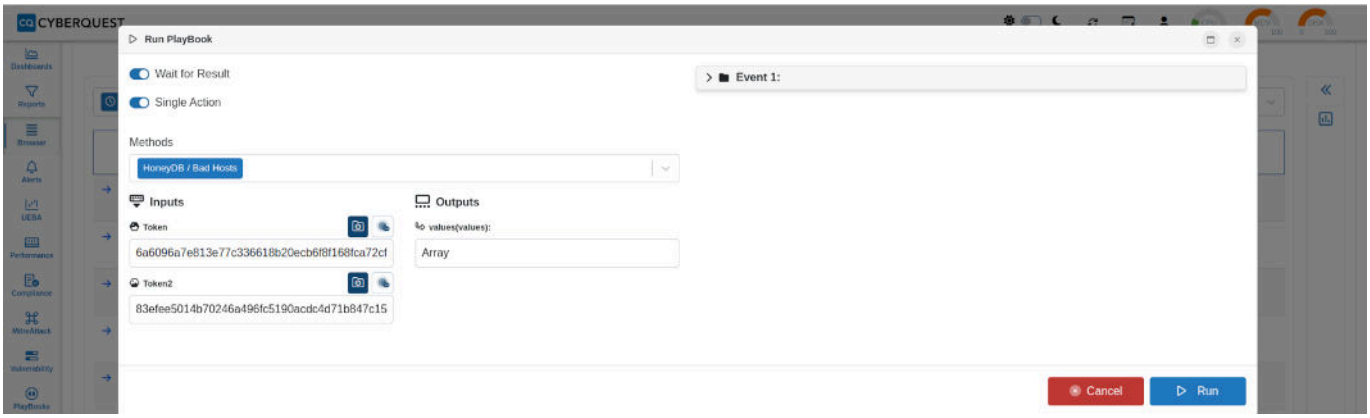
Inputs	Description
Token (is required)	To use GreyNoise API you need to have a API Key
IP (is required)	IP address to query

Outputs	Description
IP(ip)	The investigated IP
Noise(noise)	If true, this IP has been observed scanning the internet
Riot(riot)	If true, this IP was found in the RIOT project dataset
Classification(classification)	The GreyNoise classification for this IP (e.g., “malicious”)
Name(name)	Name of the Organization that owns the IP
Link(link)	A link to the GreyNoise Visualizer for that IP
Last seen(last_seen)	The last date the IP was observed by GreyNoise
Message(message)	The status of the API call

HoneyDB

HoneyDB/Bad Hosts method

Retrieve a list of bad hosts from HoneyDB.

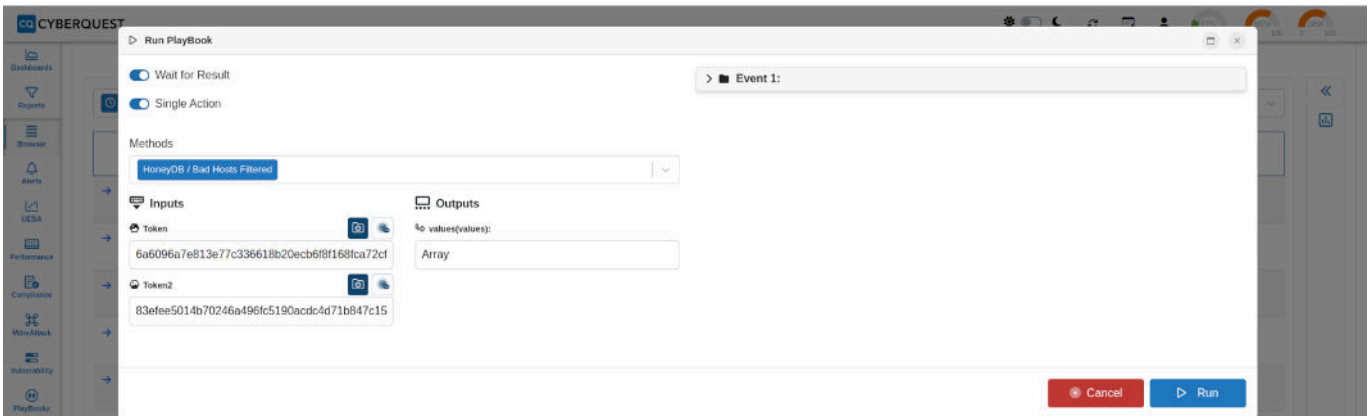


Inputs	Description
Token (is required)	The HoneyDB API ID is your identifier to use when querying HoneyDB APIs
Token2 (is required)	The threat information API key is required to query information from HoneyDB APIs.The threat information API key is required to query information from HoneyDB APIs

Outputs	Description
values(values)	The results of the API call

HoneyDB/Bad Hosts Filtered method

Returns the data provided by the user to HoneyDB and enables you to download bad-host data generated by the sensors you operate.

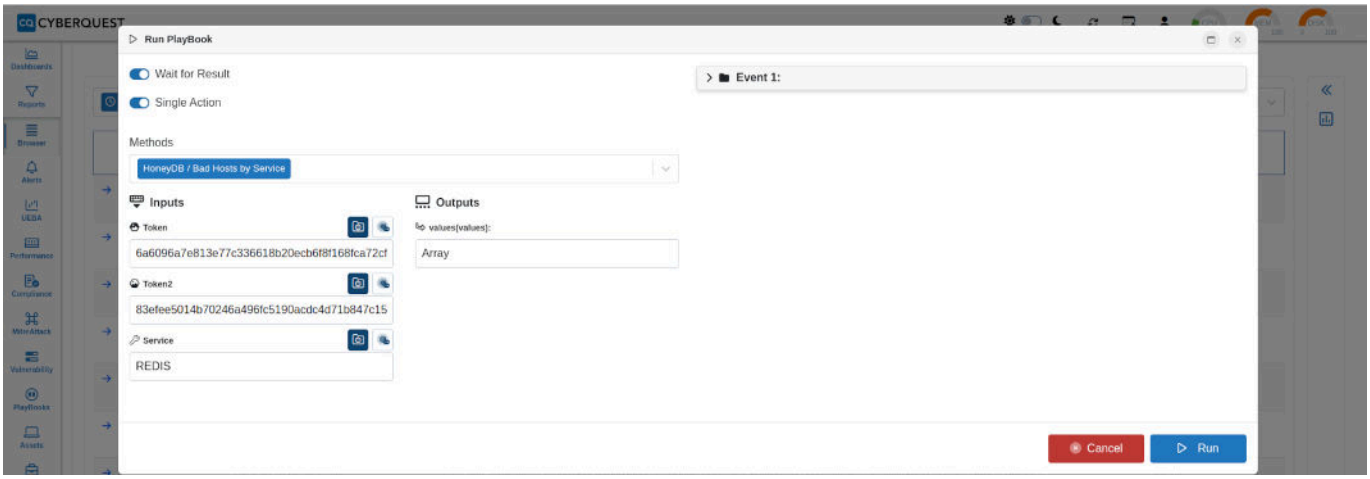


Inputs	Description
Token (is required)	The HoneyDB API ID is your identifier to use when querying HoneyDB APIs
Token2 (is required)	The threat information API key is required to query information from HoneyDB APIs

Outputs	Description
values(values)	The results of the API call

HoneyDB/Bad Hosts by Service method

Retrieve bad hosts by service name.

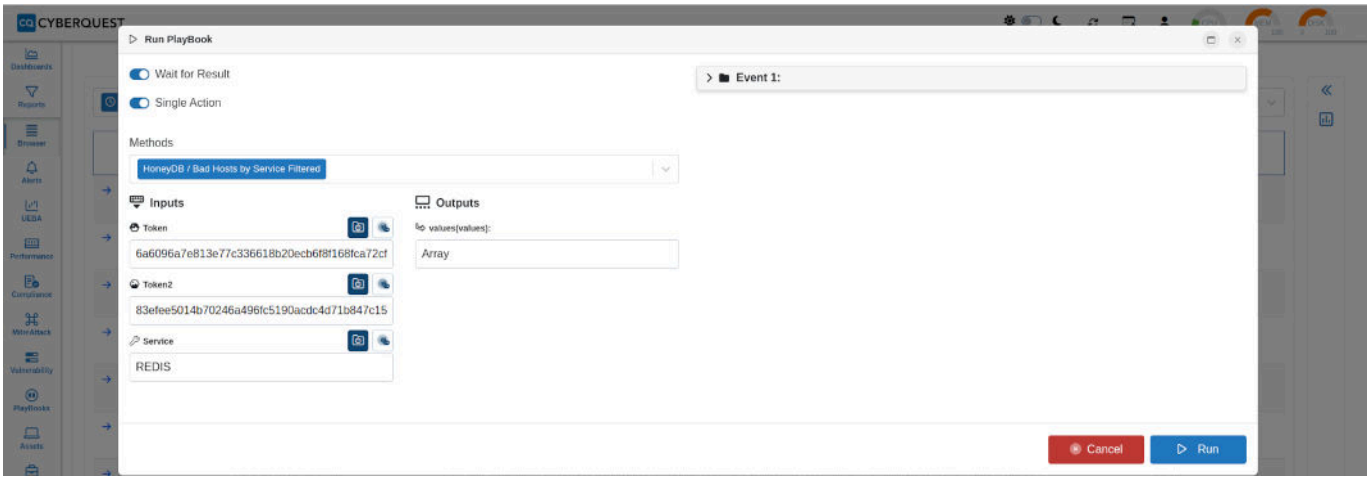


Inputs	Description
Token (is required)	The HoneyDB API ID is your identifier to use when querying HoneyDB APIs
Token2 (is required)	The threat information API key is required to query information from HoneyDB APIs
Service (is required)	Provide the service name

Outputs	Description
values(values)	The results of the API call

HoneyDB/Bad Hosts by Service Filtered method

Returns bad hosts by service name provided by the user to HoneyDB and enables you to download bad-host data, by service name, generated by the sensors you operate.

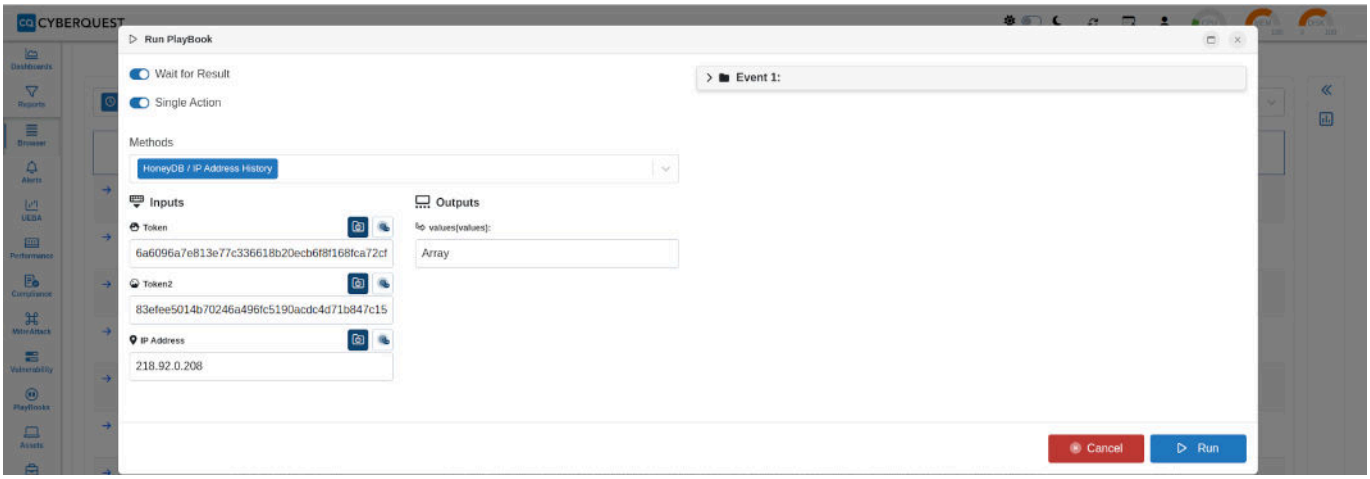


Inputs	Description
Token (is required)	The HoneyDB API ID is your identifier to use when querying HoneyDB APIs
Token2 (is required)	The threat information API key is required to query information from HoneyDB APIs
Service (is required)	Provide the service name

Outputs	Description
values(values)	The results of the API call

HoneyDB/IP Address History method

IP (bad host) history is a summary of all interaction activity for a certain IP address recorded by the HoneyDB network.

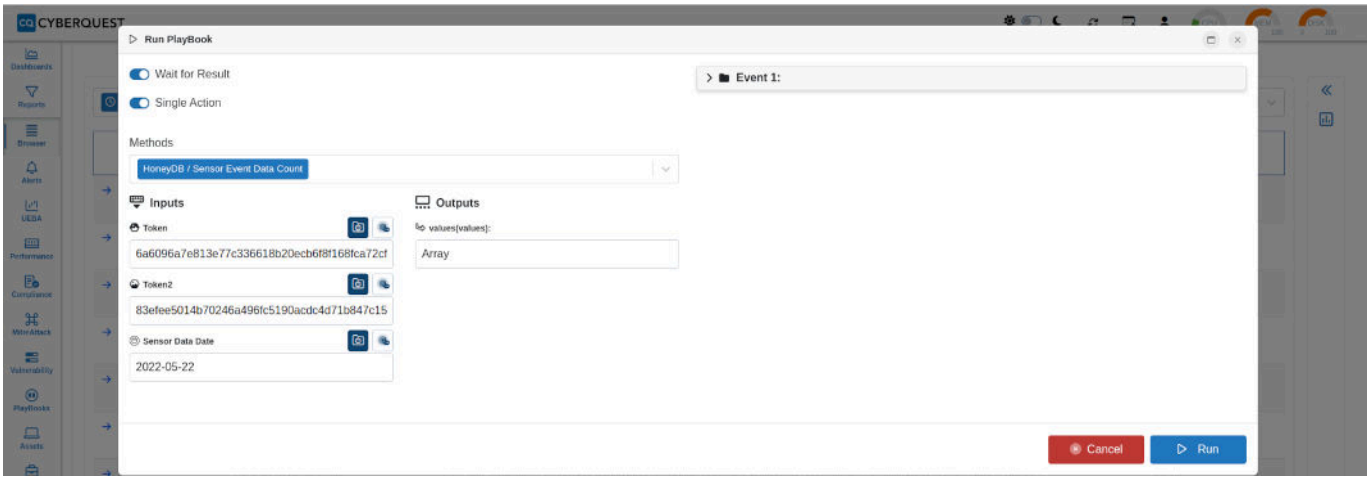


Inputs	Description
Token (is required)	The HoneyDB API ID is your identifier to use when querying HoneyDB APIs
Token2 (is required)	The threat information API key is required to query information from HoneyDB APIs
IP Address (is required)	The IP Address that is being searched

Outputs	Description
values(values)	The results of the API call

HoneyDB/Sensor Event Data Count method

If you have sensors that log data to HoneyDB, you can use this API to get a count of sensor event data collected for a specified date.

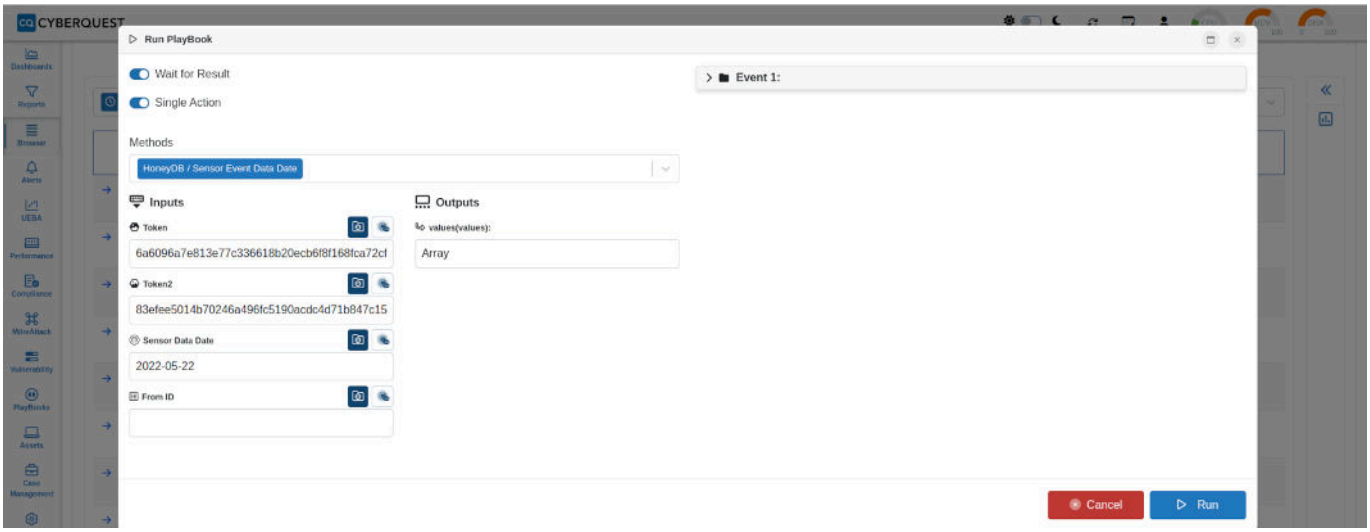


Inputs	Description
Token (is required)	The HoneyDB API ID is your identifier to use when querying HoneyDB APIs
Token2 (is required)	The threat information API key is required to query information from HoneyDB APIs
Sensor Data Date (is required)	The date on which to count events. Format: YYYY-MM-DD

Outputs	Description
values(values)	The results of the API call

HoneyDB/Sensor Event Data Date method

If you have sensors that log data to HoneyDB, you may use this endpoint to get all sensor event data collected for a specified date.

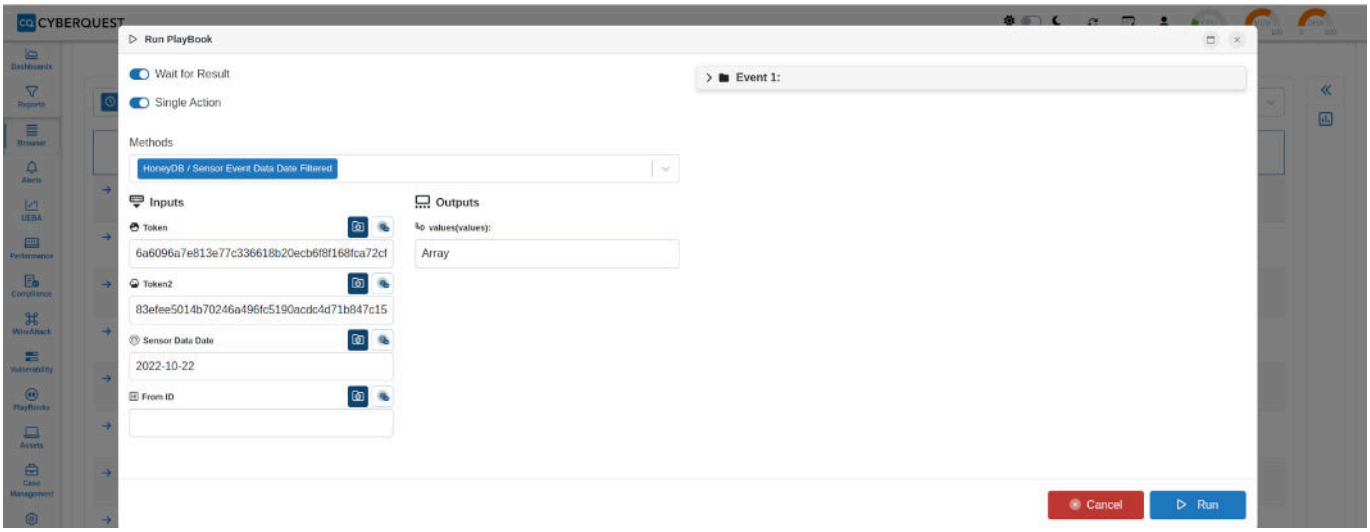


Inputs	Description
Token (is required)	The HoneyDB API ID is your identifier to use when querying HoneyDB APIs
Token2 (is required)	The threat information API key is required to query information from HoneyDB APIs
Sensor Data Date (is required)	The date on which to count events. Format: YYYY-MM-DD
From ID	The id used as a starting point to retrieve the next 1000 results

Outputs	Description
values(values)	The results of the API call

HoneyDB/Sensor Event Data Date Filtered method

If you have sensors that log data to HoneyDB, you may use this endpoint to get all your sensor event data collected for a specified date.

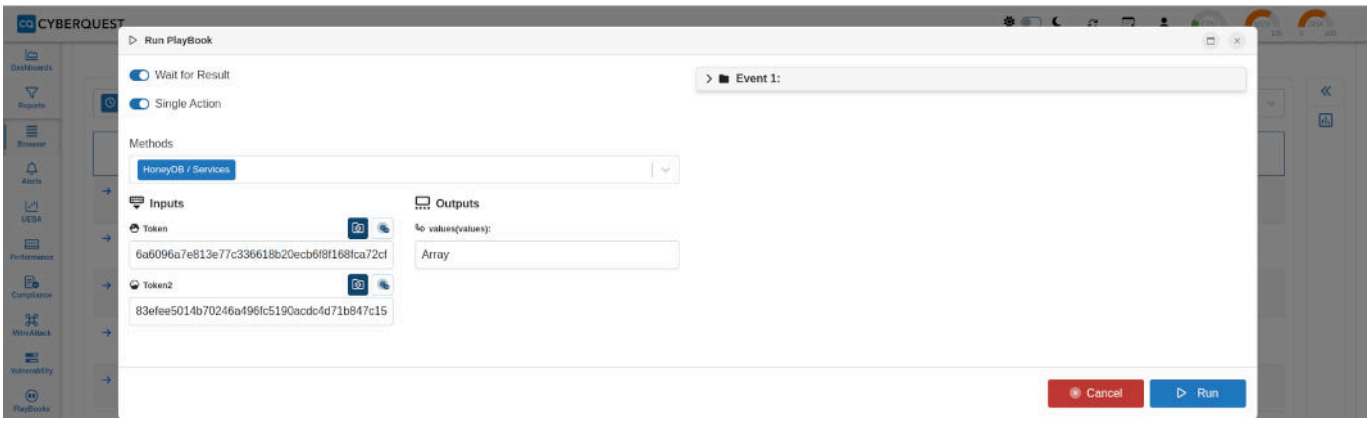


Inputs	Description
Token (is required)	The HoneyDB API ID is your identifier to use when querying HoneyDB APIs
Token2 (is required)	The threat information API key is required to query information from HoneyDB APIs
Sensor Data Date (is required)	The date on which to count events. Format: YYYY-MM-DD
From ID	The id used as a starting point to retrieve the next 1000 results

Outputs	Description
values(values)	The results of the API call

HoneyDB/Services method

Returns services which are the network protocols emulated by honeypot sensors.

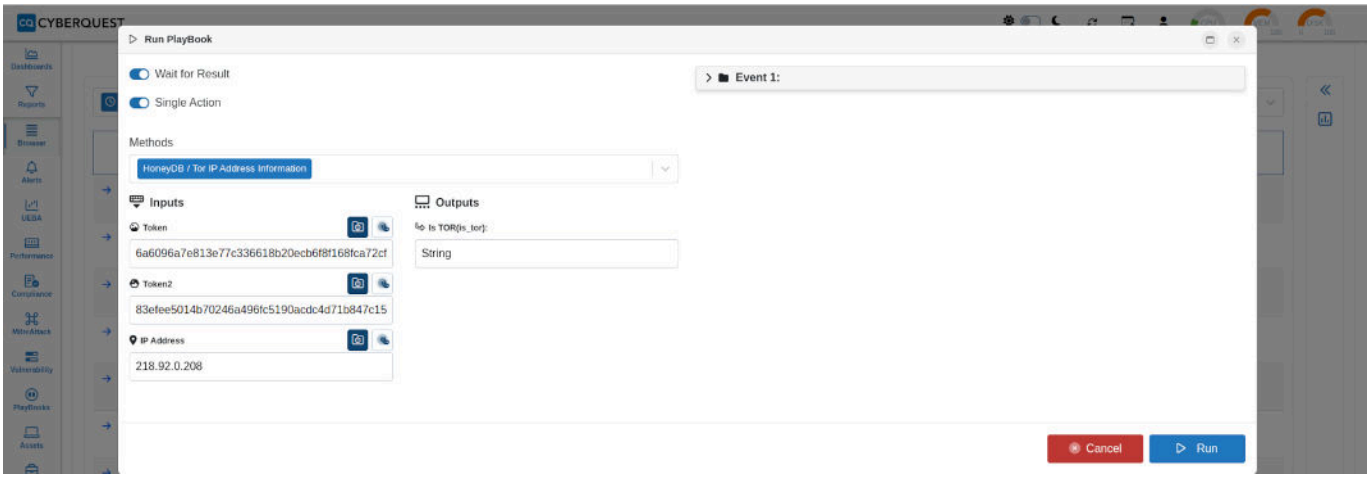


Inputs	Description
Token (is required)	The HoneyDB API ID is your identifier to use when querying HoneyDB APIs
Token2 (is required)	The threat information API key is required to query information from HoneyDB APIs

Outputs	Description
values(values)	The results of the API call

HoneyDB/Tor IP Address Information method

Returns true or false to indicate if the IP address provided is a Tor exit node.

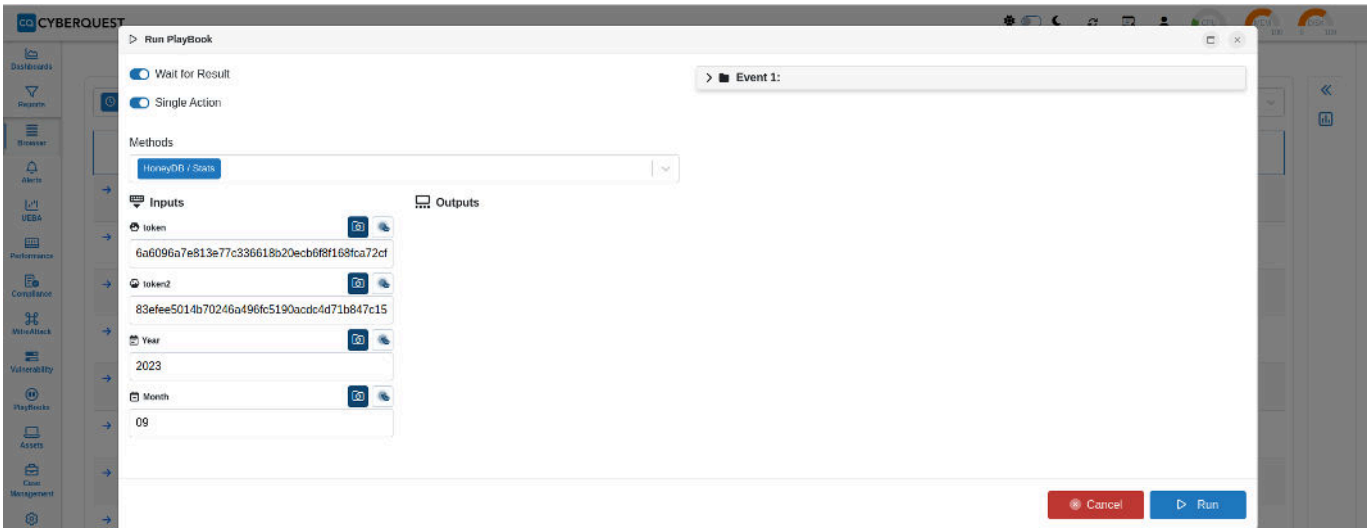


Inputs	Description
Token (is required)	The HoneyDB API ID is your identifier to use when querying HoneyDB APIs
Token2 (is required)	The threat information API key is required to query information from HoneyDB APIs
IP Address (is required)	The IP Address that is being searched

Outputs	Description
values(values)	The results of the API call

HoneyDB/Stats method

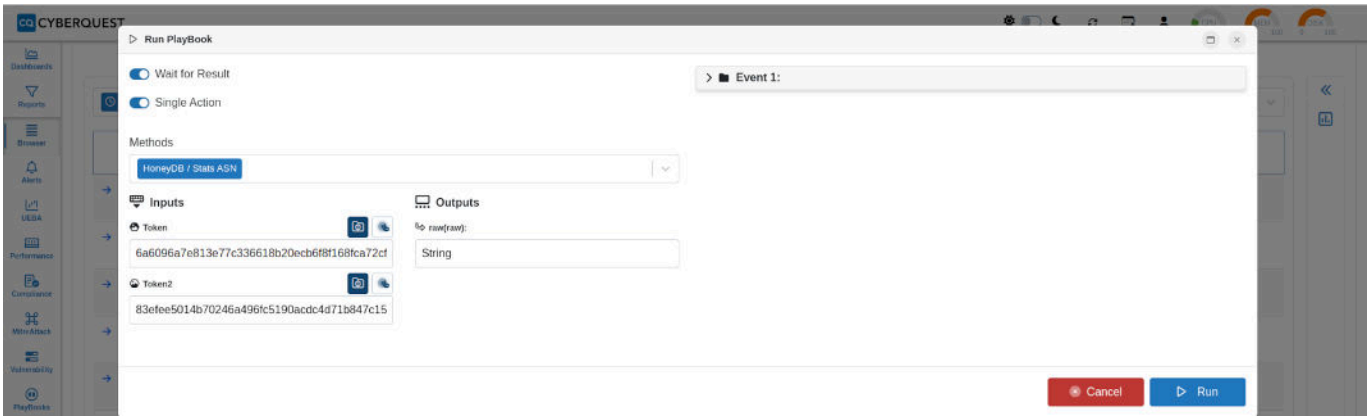
Returns services which are the network protocols emulated by honeypot sensors.



Inputs	Description
Token (is required)	The HoneyDB API ID is your identifier to use when querying HoneyDB APIs
Token2 (is required)	The threat information API key is required to query information from HoneyDB APIs
Year	The year published. Format: YYYY
Month	The month published. Format: MM

HoneyDB/Stats ASN method

Return a list of Average Sample Number.

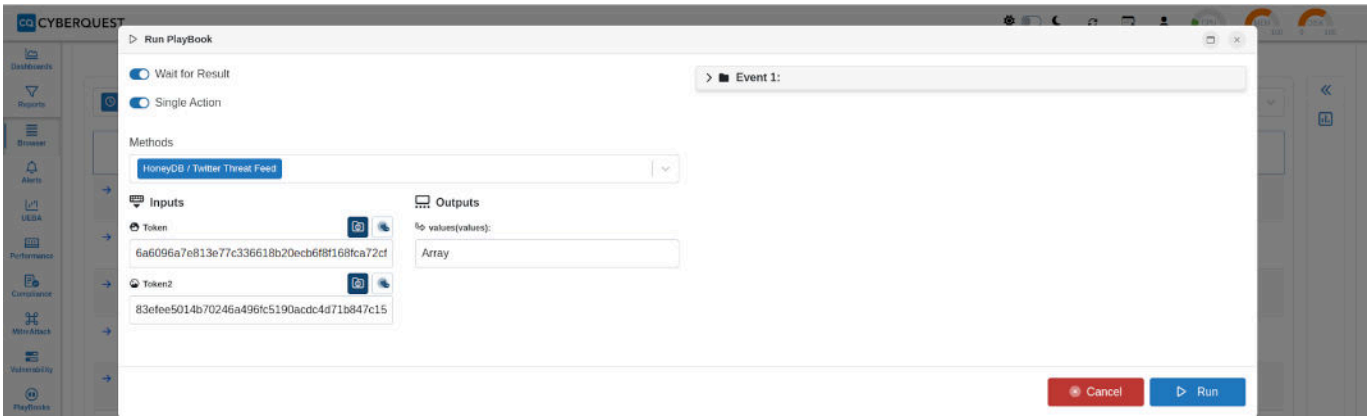


Inputs	Description
Token (is required)	The HoneyDB API ID is your identifier to use when querying HoneyDB APIs
Token2 (is required)	The threat information API key is required to query information from HoneyDB APIs

Outputs	Description
raw(raw)	The results of the API call

HoneyDB/Twitter Threat Feed method

The Twitter threat feed includes a list of problematic hosts that have connected or attempted to connect to other honeypots on the Internet (including honeypots that do not submit data directly to HoneyDB).

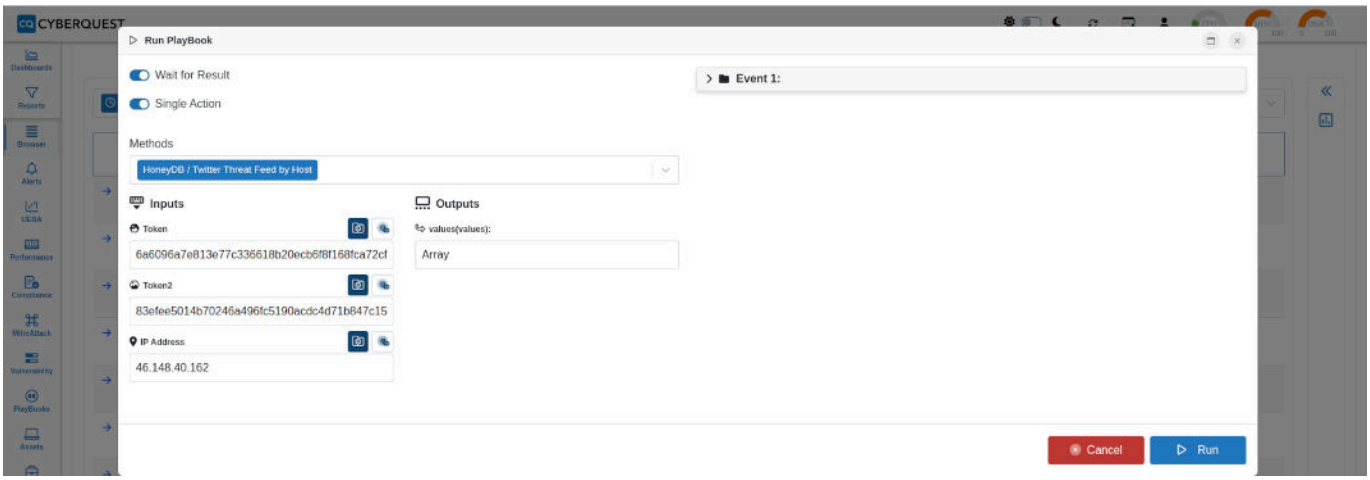


Inputs	Description
Token (is required)	The HoneyDB API ID is your identifier to use when querying HoneyDB APIs
Token2 (is required)	The threat information API key is required to query information from HoneyDB APIs

Outputs	Description
values(values)	The results of the API call

HoneyDB/Twitter Threat Feed by Host method

Twitter threat feed data filtered by host (IP address).

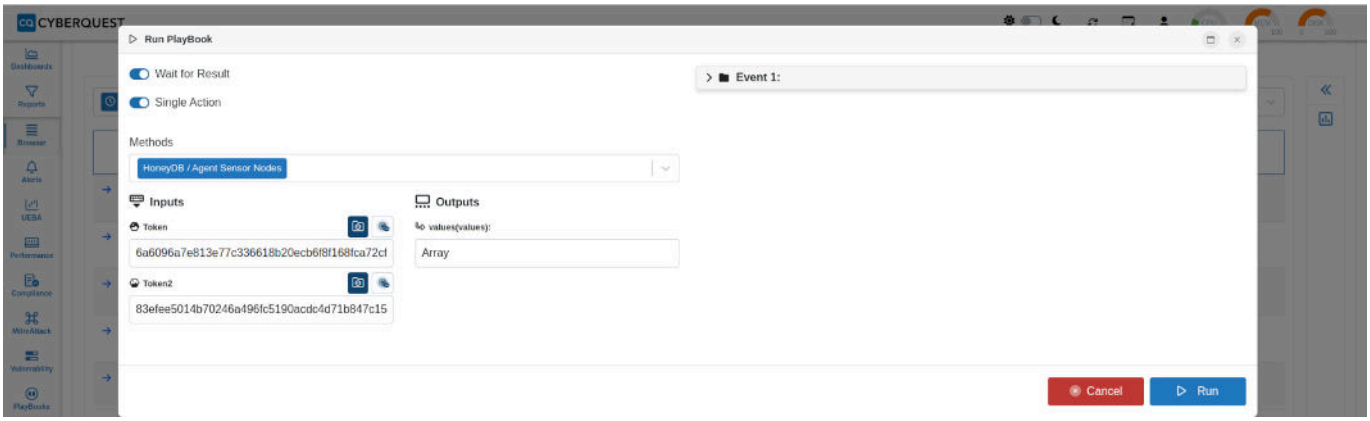


Inputs	Description
Token (is required)	The HoneyDB API ID is your identifier to use when querying HoneyDB APIs
Token2 (is required)	The threat information API key is required to query information from HoneyDB APIs
IP Address (is required)	The IP Address that is being searched

Outputs	Description
values(values)	The results of the API call

HoneyDB/Agent Sensor Nodes method

Honeydb-agent sensors are deployed on nodes. This endpoint delivers all nodes viewed within the last three days.

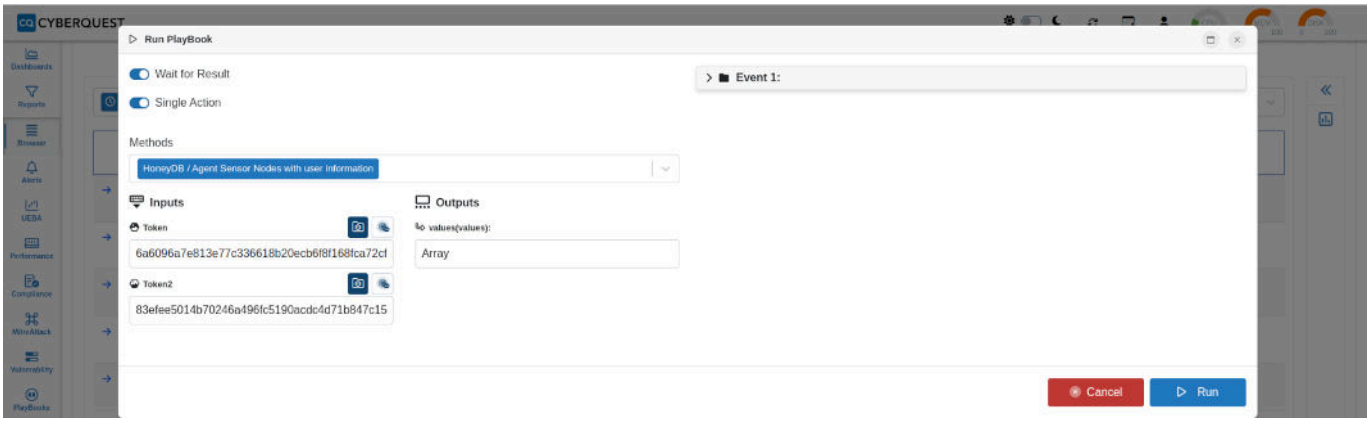


Inputs	Description
Token (is required)	The HoneyDB API ID is your identifier to use when querying HoneyDB APIs
Token2 (is required)	The threat information API key is required to query information from HoneyDB APIs

Outputs	Description
values(values)	The results of the API call

HoneyDB/Agent Sensor Nodes with user information method

Honeydb-agent sensors are deployed on nodes. This endpoint delivers all nodes viewed within the last three days. Informations provided by the user.

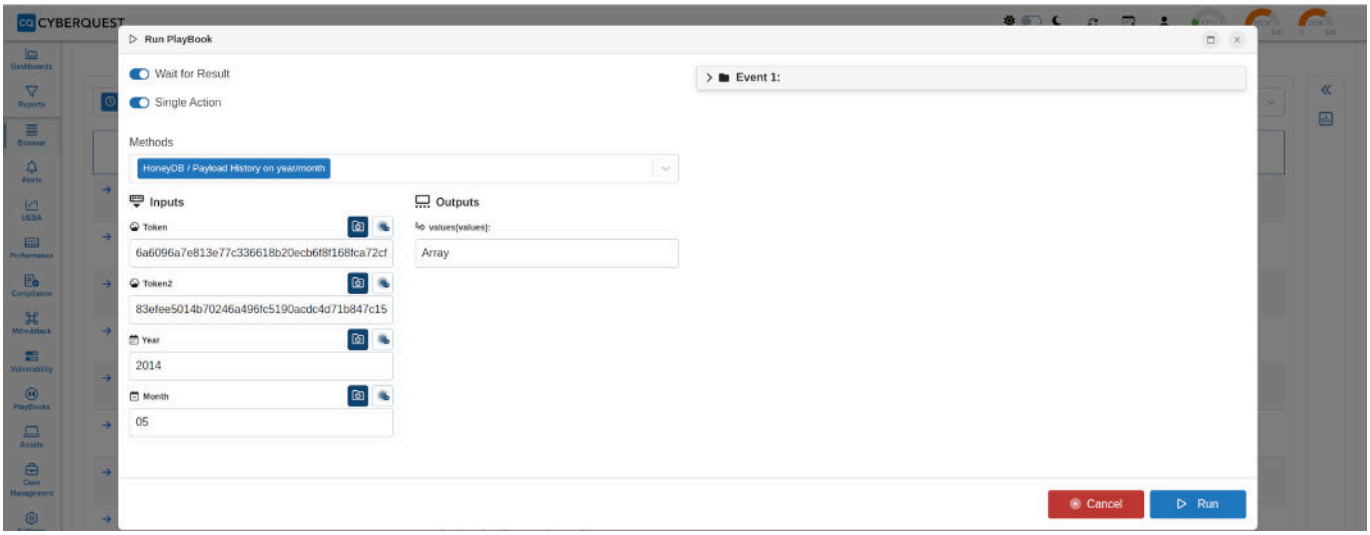


Inputs	Description
Token (is required)	The HoneyDB API ID is your identifier to use when querying HoneyDB APIs
Token2 (is required)	The threat information API key is required to query information from HoneyDB APIs

Outputs	Description
values(values)	The results of the API call

HoneyDB/Payload History on year/month method

IP (bad host) history (month with year) is a list of all interactions recorded by the HoneyDB network for a specific IP address.

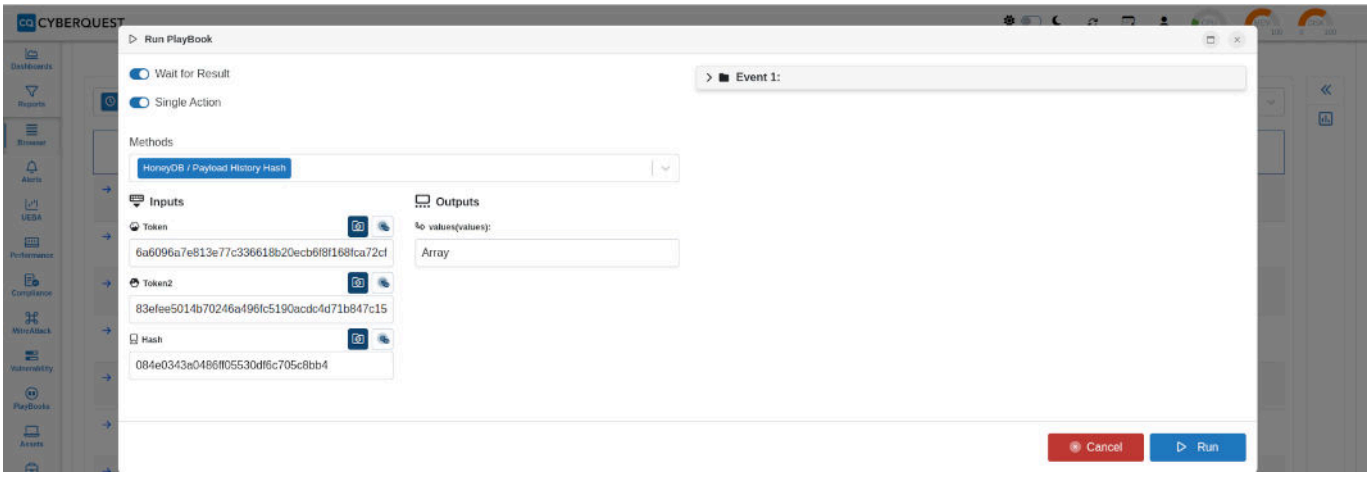


Inputs	Description
Token (is required)	The HoneyDB API ID is your identifier to use when querying HoneyDB APIs
Token2 (is required)	The threat information API key is required to query information from HoneyDB APIs
Year (is required)	The year from which you want to receive results
Month (is required)	The month from which you want to receive results

Outputs	Description
values(values)	The results of the API call

HoneyDB/Payload History Hash method

IP (bad host) history (hash) is a list of all interactions recorded by the HoneyDB network for a specific IP address.

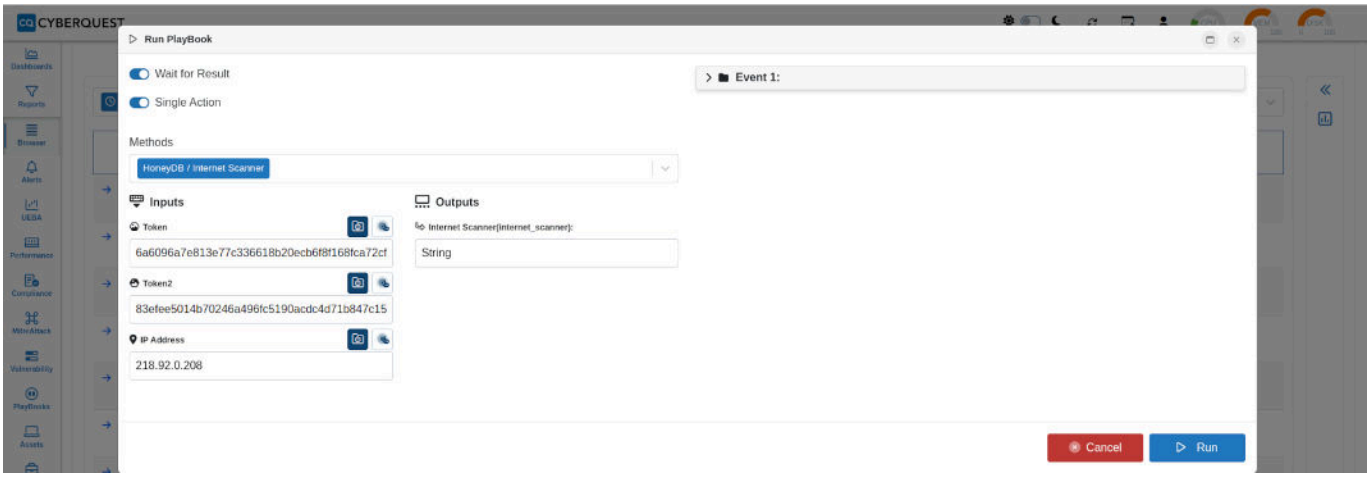


Inputs	Description
Token (is required)	The HoneyDB API ID is your identifier to use when querying HoneyDB APIs
Token2 (is required)	The threat information API key is required to query information from HoneyDB APIs
Hash (is required)	Payload hash (unique identifier)

Outputs	Description
values(values)	The results of the API call

HoneyDB/Internet Scanner method

Returns true or false depending on if the provided IP address is part of a known Internet scanning service.

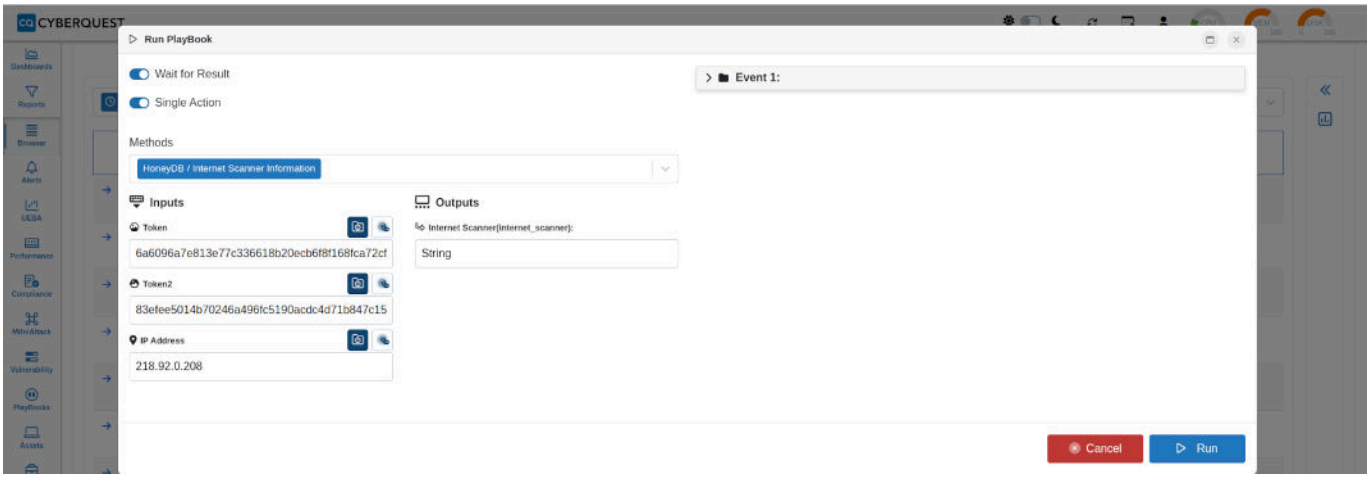


Inputs	Description
Token (is required)	The HoneyDB API ID is your identifier to use when querying HoneyDB APIs
Token2 (is required)	The threat information API key is required to query information from HoneyDB APIs
IP Address (is required)	The IP Address that is being searched

Outputs	Description
Internet Scanner(internet_scanner)	True if the investigated IP is part of a known Internet scanning service, otherwise false

HoneyDB/Internet Scanner Information method

Returns true or false to indicate if the IP provided is part of a known Internet scanning service as well as additional information about the scanning entity.

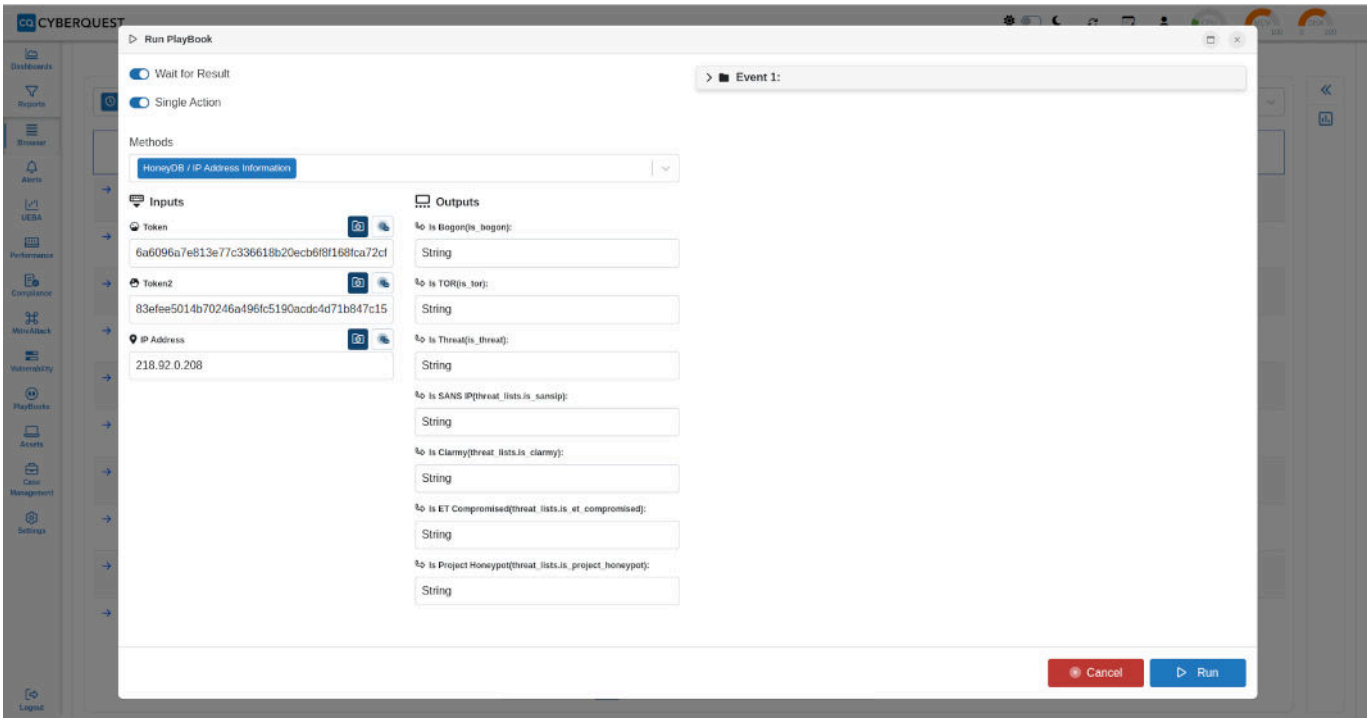


Inputs	Description
Token (is required)	The HoneyDB API ID is your identifier to use when querying HoneyDB APIs
Token2 (is required)	The threat information API key is required to query information from HoneyDB APIs
IP Address (is required)	The IP Address that is being searched

Outputs	Description
Internet Scanner(internet_scanner)	True if the investigated IP is part of a known Internet scanning service, otherwise false

HoneyDB/IP Address Information method

Returns true or false to show whether the provided IP address is on a known IP list.

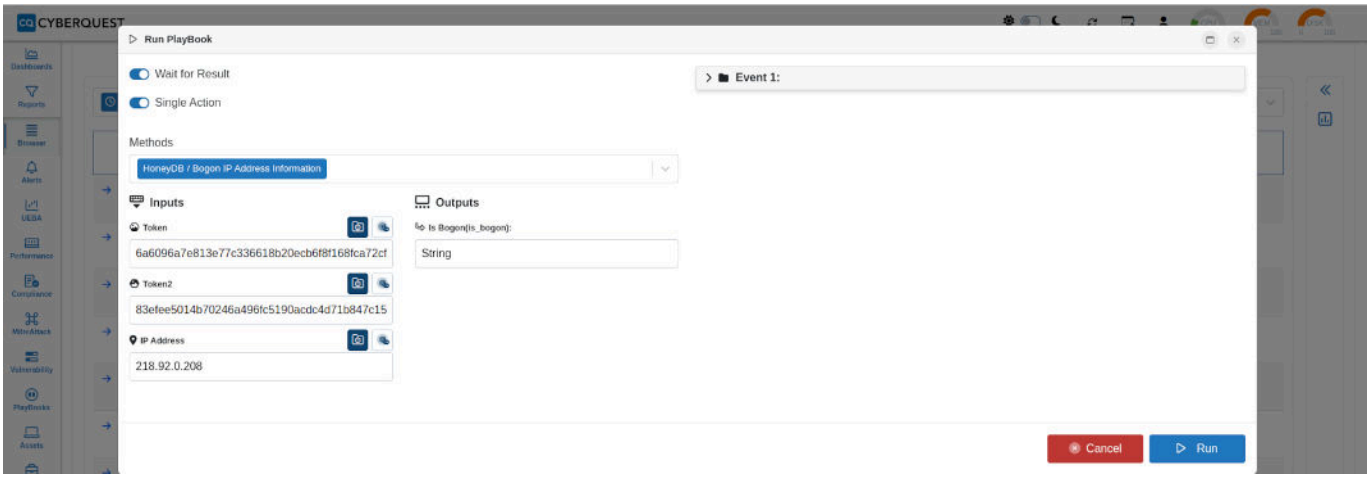


Inputs	Description
Token (is required)	The HoneyDB API ID is your identifier to use when querying HoneyDB APIs
Token2 (is required)	The threat information API key is required to query information from HoneyDB APIs
IP Address (is required)	The IP Address that is being searched

Outputs	Description
Is Bogon(is_bogon)	True if the investigated IP is Bogon, otherwise false
Is TOR(is_tor)	True if the investigated IP is TOR, otherwise false
Is Threat(is_threat)	True if the investigated IP is a Threat, otherwise false
Is SANS IP(threat_lists.is_sansip)	True if the investigated IP is from SANS, otherwise false
Is Ciarmy(threat_lists.is_ciarmy)	True if the investigated IP is from Ciarmy, otherwise false
Is ET Compromised(threat_lists.is_et_compromised)	True if the investigated IP is from ET Compromised, otherwise false
Is Project Honeypot(threat_lists.is_project_honeypot)	True if the investigated IP is part of a Honeypot Project, otherwise false

HoneyDB/Bogon IP Address Information method

Returns true or false to indicate if the IP provided is bogon IP address.

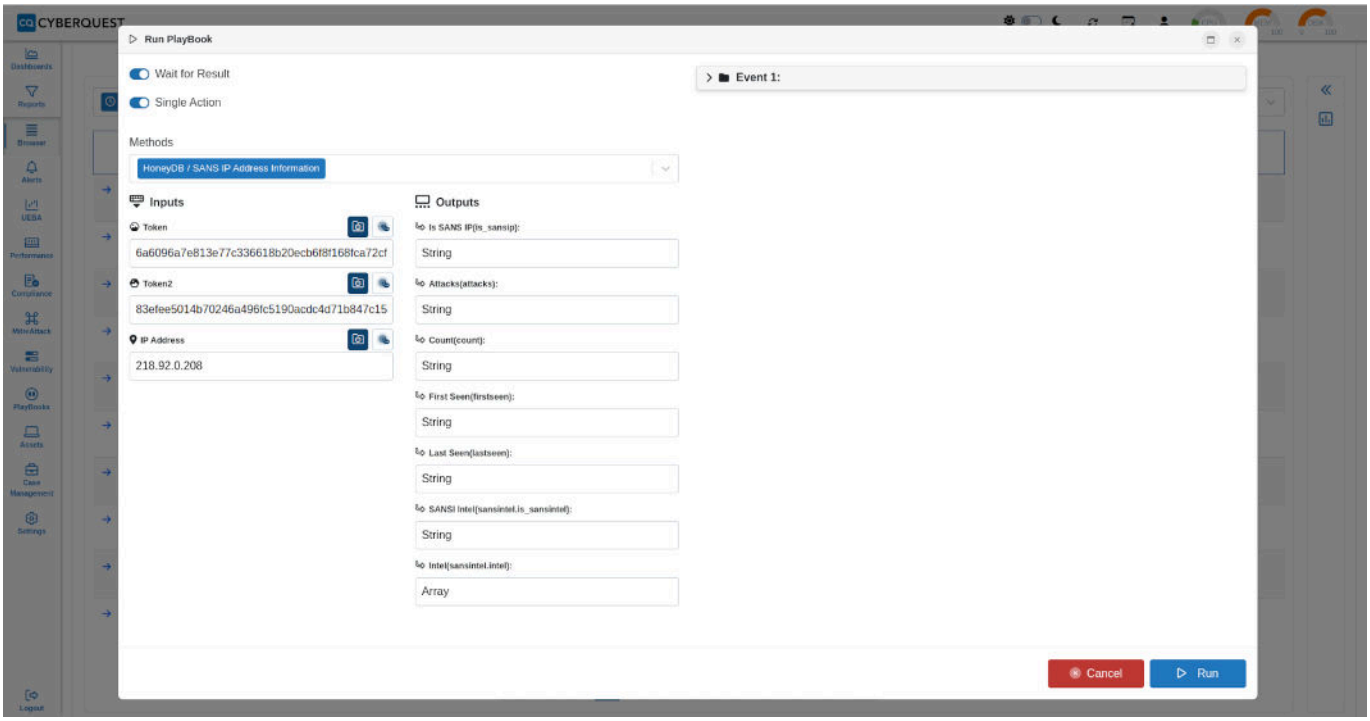


Inputs	Description
Token (is required)	The HoneyDB API ID is your identifier to use when querying HoneyDB APIs
Token2 (is required)	The threat information API key is required to query information from HoneyDB APIs
IP Address (is required)	The IP Address that is being searched

Outputs	Description
Is Bogon(is_bogon)	True if the investigated IP is Bogon, otherwise false

HoneyDB/SANS IP Address Information method

Returns true or false to indicate if the IP provided is on the SANS IP list.

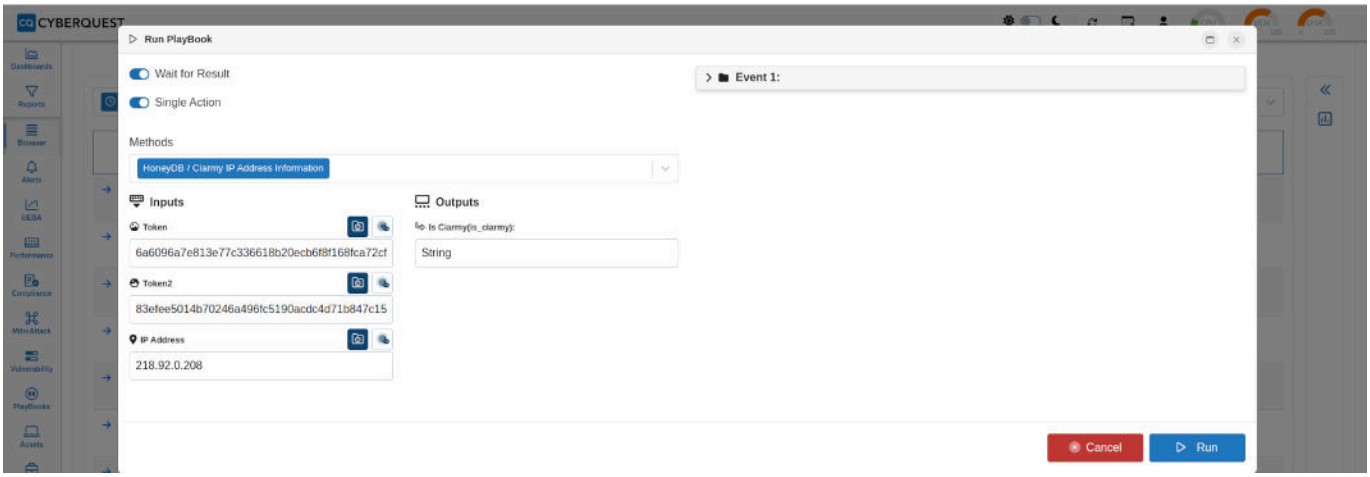


Inputs	Description
Token (is required)	The HoneyDB API ID is your identifier to use when querying HoneyDB APIs
Token2 (is required)	The threat information API key is required to query information from HoneyDB APIs
IP Address (is required)	The IP Address that is being searched

Outputs	Description
Is SANS IP(is_sansip)	True if the investigated IP is from SANS, otherwise false
Attacks(attacks)	The attack where the investigated IP was seen
Count(count)	The number of attacks
First Seen(firstseen)	The timestamp when the investigated IP was first time seen
Last Seen(lastseen)	The timestamp when the investigated IP was last time seen
SANSI Intel(sansintel.is_sansintel)	True if the investigated IP is part of SANSI Intel
Intel(sansintel.intel)	The details about the investigated IP

HoneyDB/Ciarmy IP Address Information method

Returns true or false to indicate if the IP provided is on the The CINS Army List.

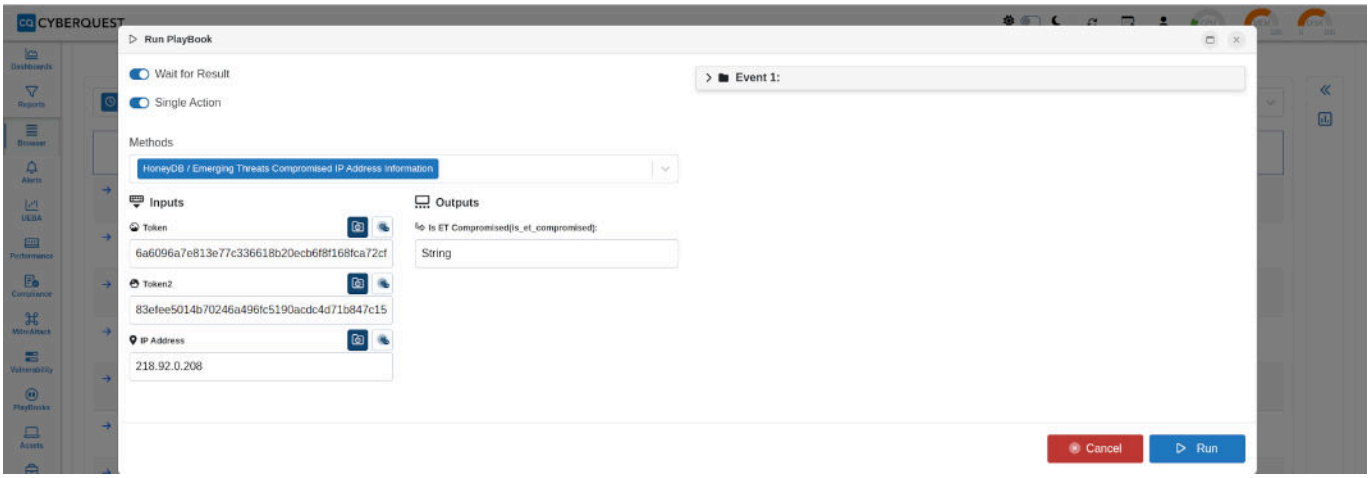


Inputs	Description
Token (is required)	The HoneyDB API ID is your identifier to use when querying HoneyDB APIs
Token2 (is required)	The threat information API key is required to query information from HoneyDB APIs
IP Address (is required)	The IP Address that is being searched

Outputs	Description
Is Ciarmy(is_ciarmy)	True if the investigated IP is from Ciarmy, otherwise false

HoneyDB/Emerging Threats Compromised IP Address Information method

Returns true or false to indicate if the IP provided is on the Emerging Threats Compromised IP list.

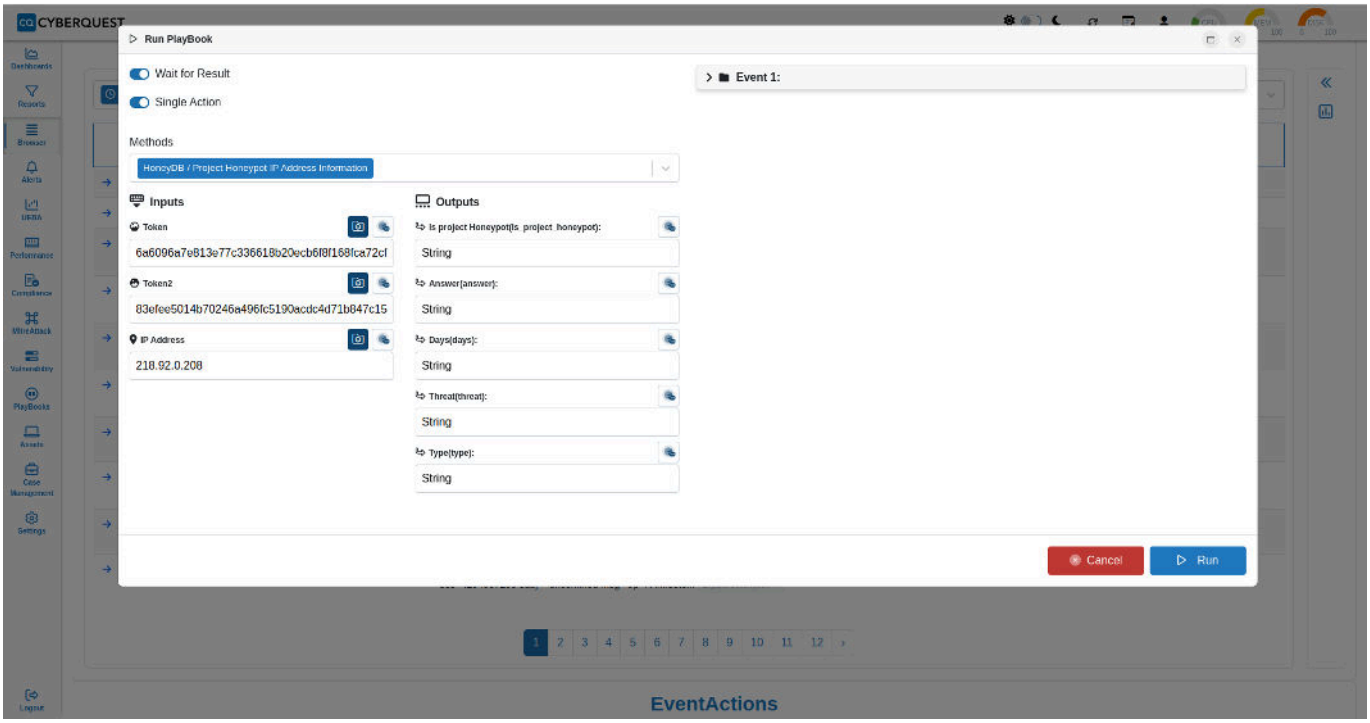


Inputs	Description
Token (is required)	The HoneyDB API ID is your identifier to use when querying HoneyDB APIs
Token2 (is required)	The threat information API key is required to query information from HoneyDB APIs
IP Address (is required)	The IP Address that is being searched

Outputs	Description
Is ET Compromised(is_et_compromised)	True if the investigated IP is from ET Compromised, otherwise false

HoneyDB/Project Honeypot IP Address Information method

Returns true or false to indicate if the IP provided is on the Project Honeypot list and additional threat data.

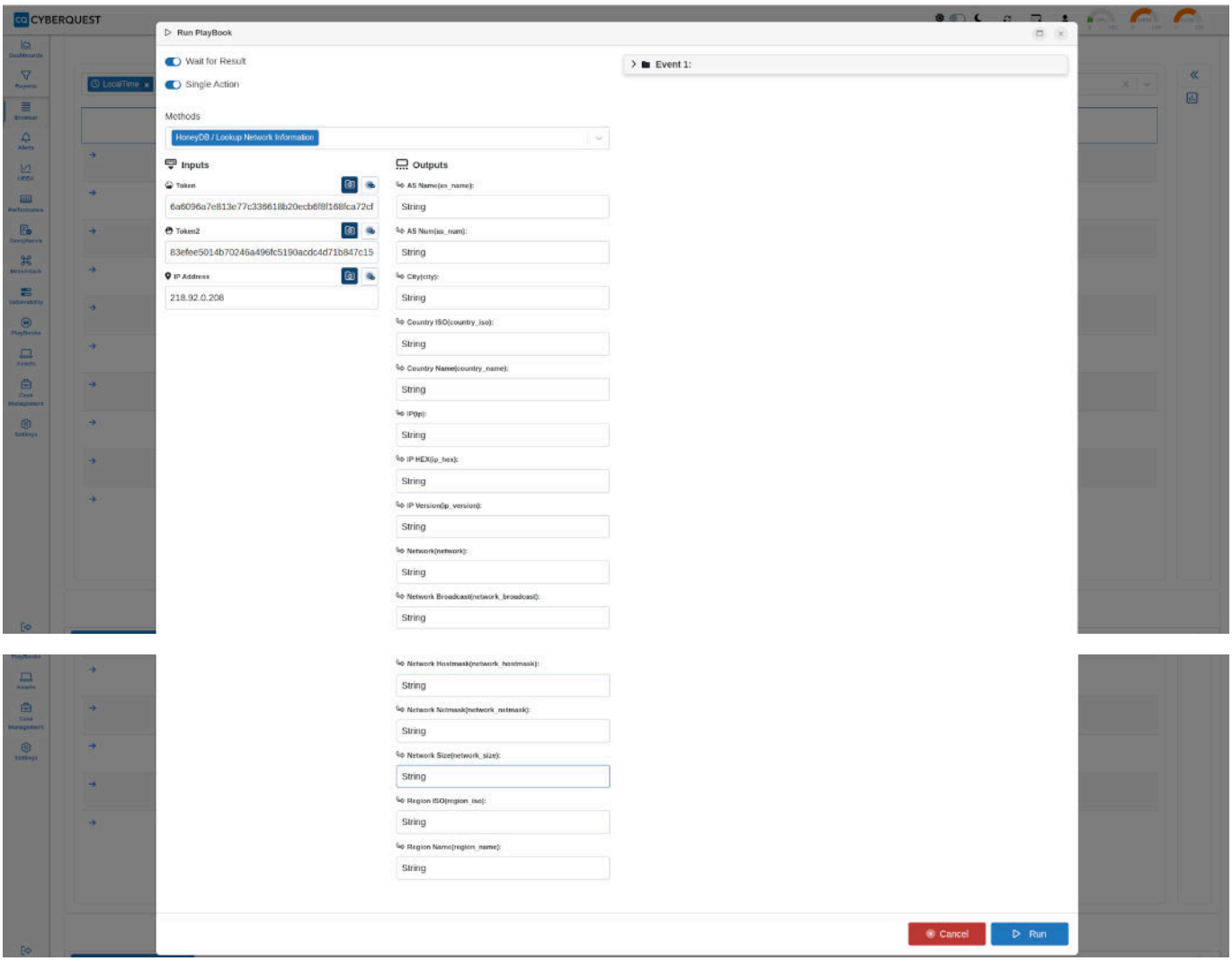


Inputs	Description
Token (is required)	The HoneyDB API ID is your identifier to use when querying HoneyDB APIs
Token2 (is required)	The threat information API key is required to query information from HoneyDB APIs
IP Address (is required)	The IP Address that is being searched

Outputs	Description
Is project Honeypot(is_project_honeypot)	True if the investigated IP is part of a Honeypot Project, otherwise false
Answer(answer)	Additional Threat Data
Days(days)	Additional Threat Data
Threat(threat)	The category where is classified the investigated IP
Type(type)	The type of threat

HoneyDB/Lookup Network Information method

Returns AS, network information and geolocation for an IP address.

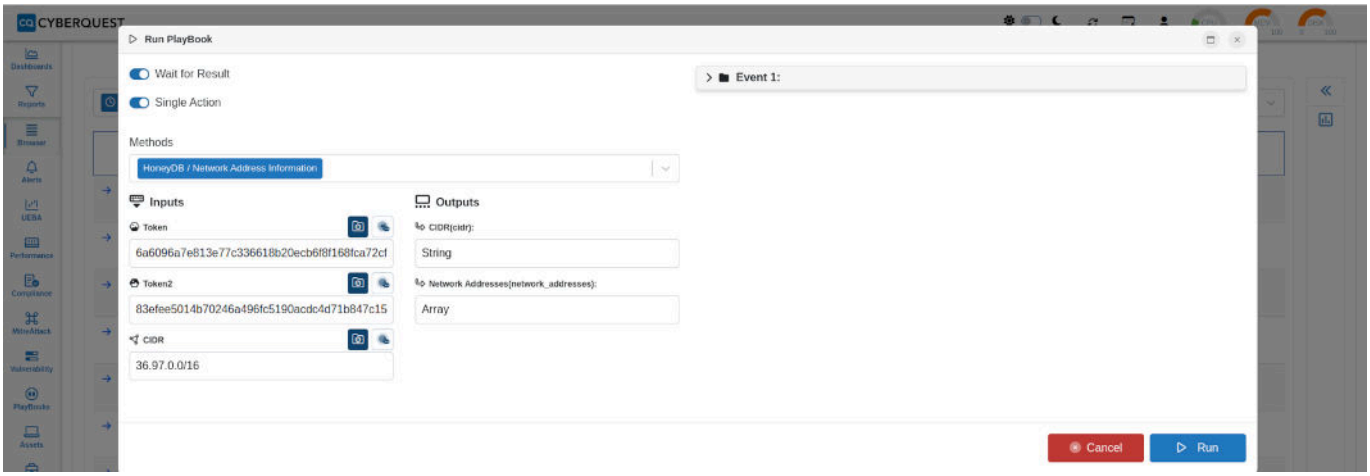


Inputs	Description
Token (is required)	The HoneyDB API ID is your identifier to use when querying HoneyDB APIs
Token2 (is required)	The threat information API key is required to query information from HoneyDB APIs
IP Address (is required)	The IP Address that is being searched

Outputs	Description
AS Name(as_name)	The AS name where of the investigated IP
AS Num(as_num)	The AS number where of the investigated IP
City(city)	The city where is located the investigated IP
Country ISO(country_iso)	The ISO country code where is located the investigated IP
Country Name(country_name)	The country name where is located the investigated IP
IP(ip)	The investigated IP
IP HEX(ip_hex)	The investigated IP in hexadecimal format
IP Version(ip_version)	The version fo the investigated IP
Network(network)	The network of the investigated IP
Network Broadcast(network_broadcast)	The broadcast network of the investigated IP
Network Hostmask(network_hostmask)	The hostmask network of the investigated IP
Network Netmask(network_netmask)	The netmask network of the investigated IP
Network Size(network_size)	The size of network of the investigated IP
Region ISO(region_iso)	The ISO Region name where is located the investigated IP
Region Name(region_name)	The region name where is located the investigated IP

HoneyDB/Network Address Information method

Returns all IP addresses as part of a network range.

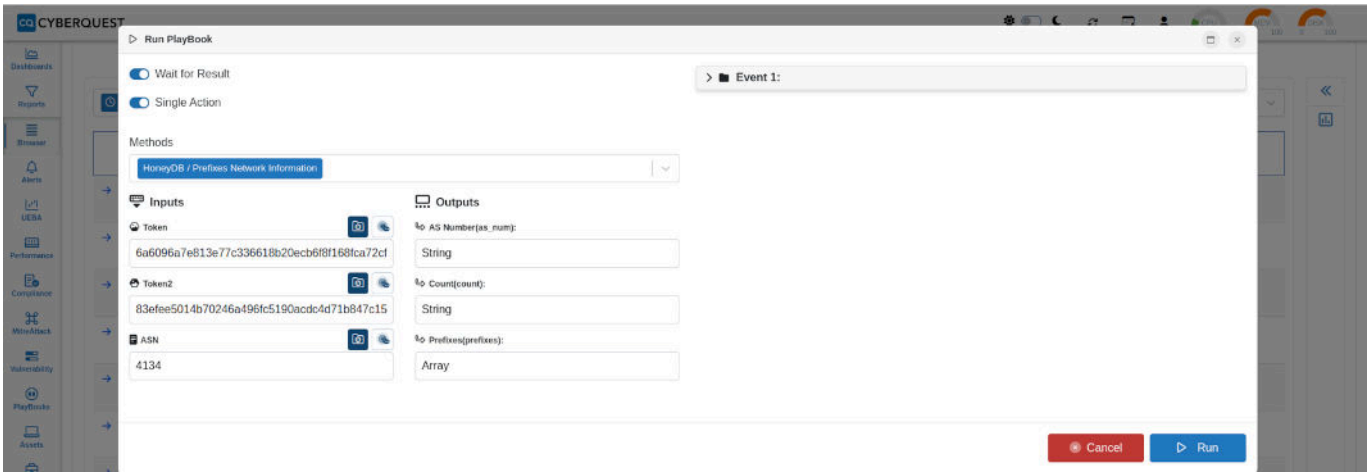


Inputs	Description
Token (is required)	The HoneyDB API ID is your identifier to use when querying HoneyDB APIs
Token2 (is required)	The threat information API key is required to query information from HoneyDB APIs
CIDR (is required)	The Classless Inter-Domain Routing (CIDR) that is being searched

Outputs	Description
CIDR(cidr)	The CIDR Value
Network Addresses(network_addresses)	A list of network addresses

HoneyDB/Prefixes Network Information method

Returns all prefixes advertised for a specific Autonomous System (AS) network.

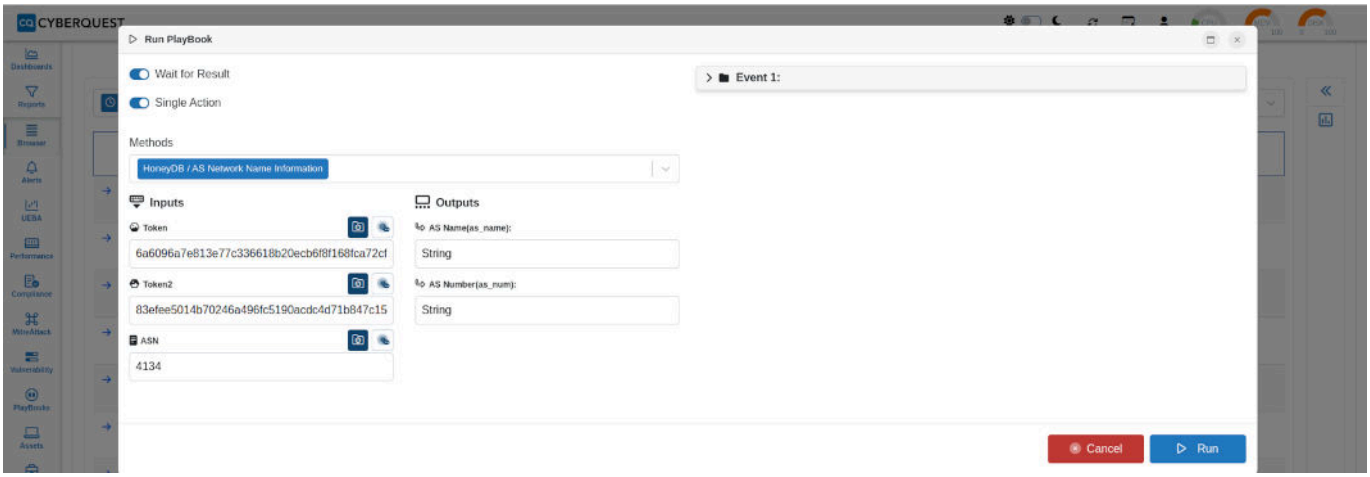


Inputs	Description
Token (is required)	The HoneyDB API ID is your identifier to use when querying HoneyDB APIs
Token2 (is required)	The threat information API key is required to query information from HoneyDB APIs
ASN (is required)	The ASN that is being searched

Outputs	Description
AS Number(as_num)	The investigated AS number
Count(count)	The number of prefixes
Prefixes(prefixes)	A list of prefixes that resulted from the API call

HoneyDB/AS Network Name Information method

Returns the name of the Autonomous System (AS) network.

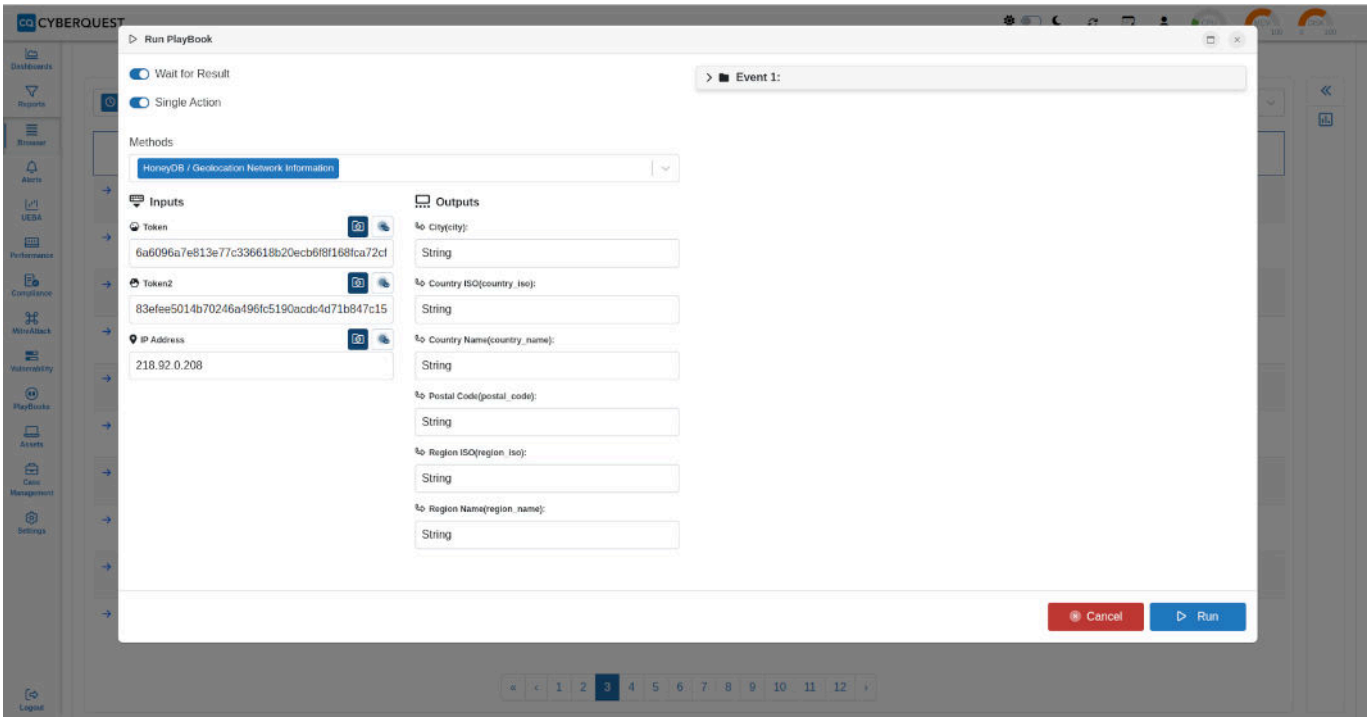


Inputs	Description
Token (is required)	The HoneyDB API ID is your identifier to use when querying HoneyDB APIs
Token2 (is required)	The threat information API key is required to query information from HoneyDB APIs
ASN (is required)	The ASN that is being searched

Outputs	Description
AS Name(as_name)	The name of the AS
AS Number(as_num)	The investigated AS number

HoneyDB/Geolocation Network Information method

Geolocation information for an IP address is returned.

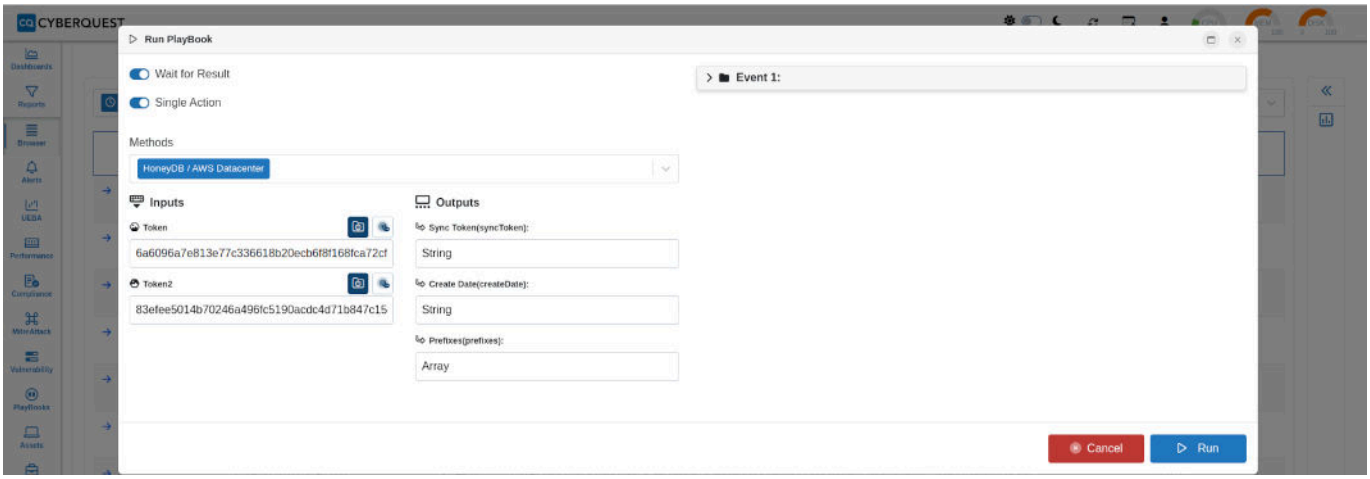


Inputs	Description
Token (is required)	The HoneyDB API ID is your identifier to use when querying HoneyDB APIs
Token2 (is required)	The threat information API key is required to query information from HoneyDB APIs
IP Address (is required)	The IP Address that is being searched

Outputs	Description
City(city)	The city where is located the investigated IP
Country ISO(country_iso)	The ISO country code where is located the investigated IP
Country Name(country_name)	The country name where is located the investigated IP
Postal Code(postal_code)	The postal code where is located the investigated IP
Region ISO(region_iso)	The ISO Region name where is located the investigated IP
Region Name(region_name)	The region name where is located the investigated IP

HoneyDB/AWS Datacenter method

Returns AWS IP address ranges.

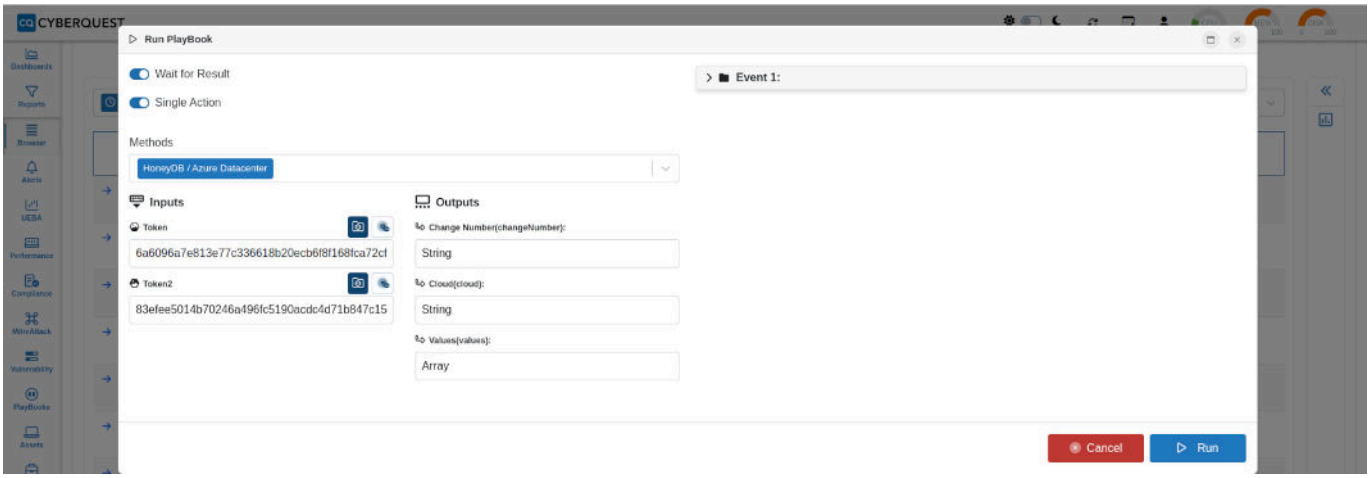


Inputs	Description
Token (is required)	The HoneyDB API ID is your identifier to use when querying HoneyDB APIs
Token2 (is required)	The threat information API key is required to query information from HoneyDB APIs

Outputs	Description
Sync Token(syncToken)	The synchronization token
Create Date(createDate)	The timestamp when the Sync Token was created
Prefixes(prefixes)	A list of prefixes that resulted from the API call

HoneyDB/Azure Datacenter method

Returns Azure IP address ranges.

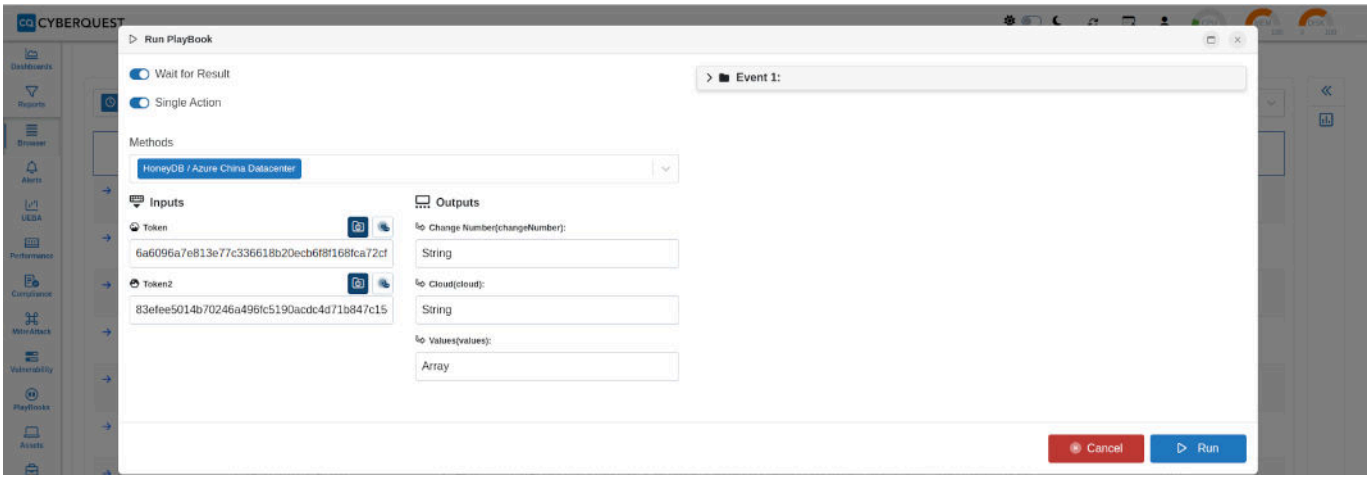


Inputs	Description
Token (is required)	The HoneyDB API ID is your identifier to use when querying HoneyDB APIs
Token2 (is required)	The threat information API key is required to query information from HoneyDB APIs

Outputs	Description
Change Number(changeNumber)	The value of the change number
Cloud(cloud)	The Cloud name
Values(values)	Details about the cloud

HoneyDB/Azure China Datacenter method

Returns Azure China IP address ranges.

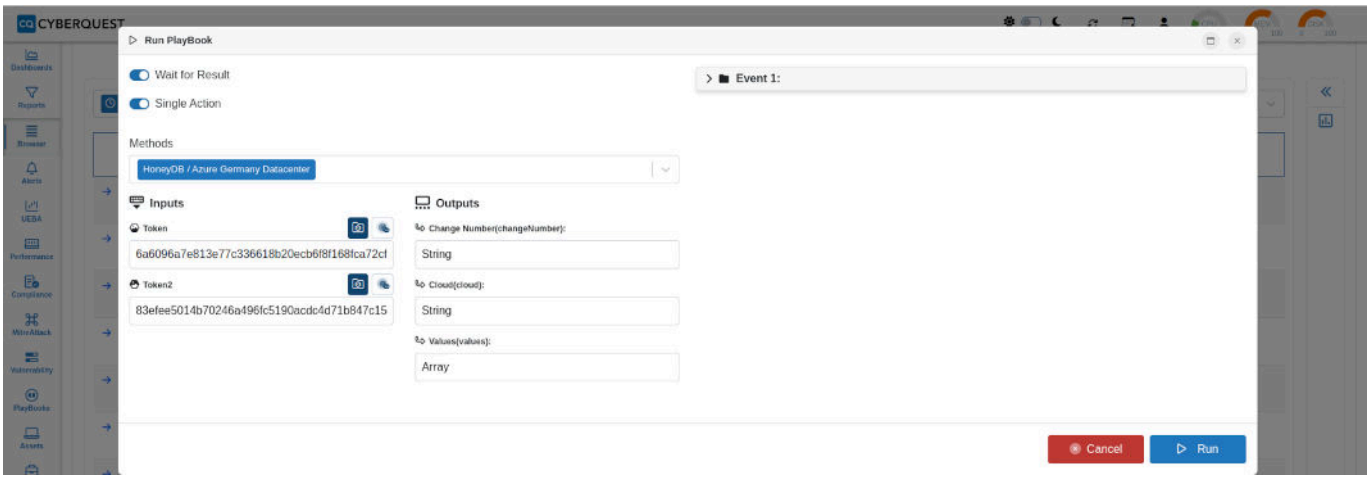


Inputs	Description
Token (is required)	The HoneyDB API ID is your identifier to use when querying HoneyDB APIs
Token2 (is required)	The threat information API key is required to query information from HoneyDB APIs

Outputs	Description
Change Number(changeNumber)	The value of the change number
Cloud(cloud)	The Cloud name
Values(values)	Details about the cloud

HoneyDB/Azure Germany Datacenter method

Returns Azure Germany IP address ranges.

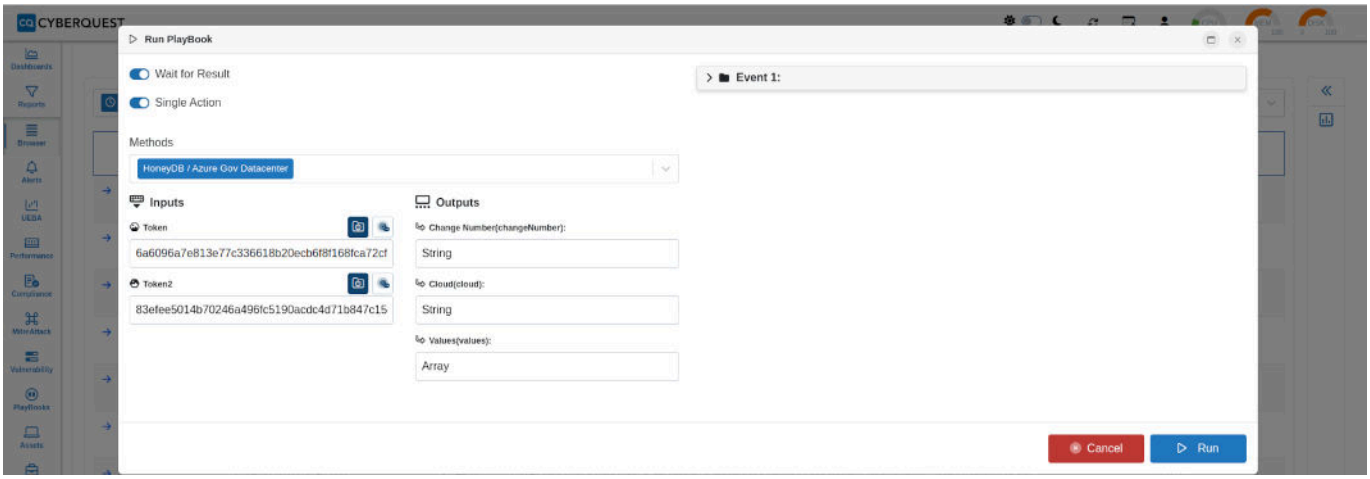


Inputs	Description
Token (is required)	The HoneyDB API ID is your identifier to use when querying HoneyDB APIs
Token2 (is required)	The threat information API key is required to query information from HoneyDB APIs

Outputs	Description
Change Number(changeNumber)	The value of the change number
Cloud(cloud)	The Cloud name
Values(values)	Details about the cloud

HoneyDB/Azure Gov Datacenter method

Returns Azure Gov IP address ranges.

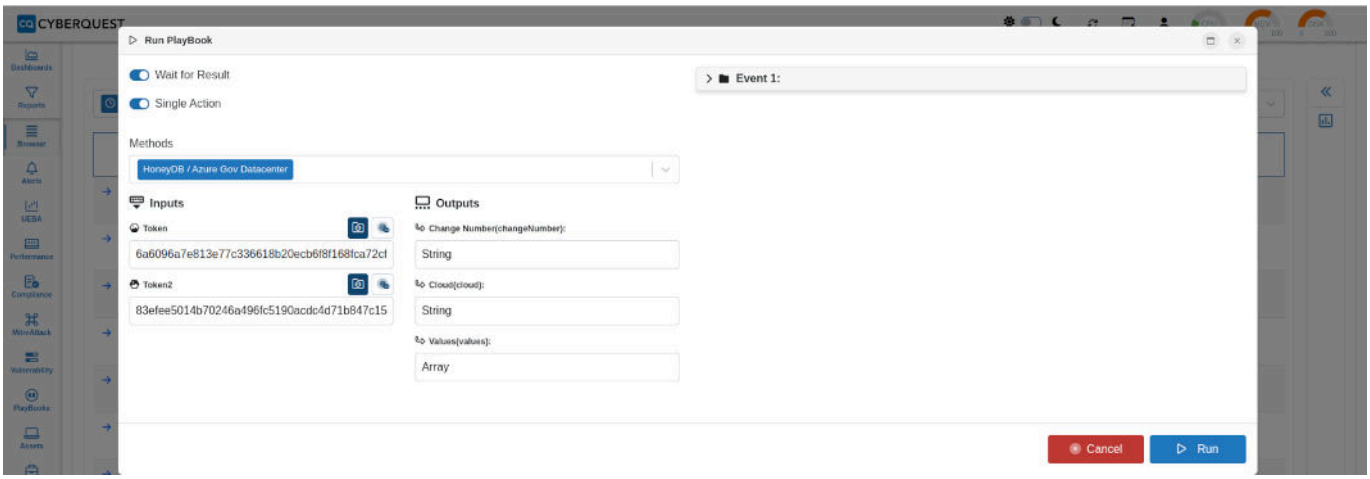


Inputs	Description
Token (is required)	The HoneyDB API ID is your identifier to use when querying HoneyDB APIs
Token2 (is required)	The threat information API key is required to query information from HoneyDB APIs

Outputs	Description
Change Number(changeNumber)	The value of the change number
Cloud(cloud)	The Cloud name
Values(values)	Details about the cloud

HoneyDB/Google Cloud Platform Datacenter method

Returns Google Cloud IP address ranges.

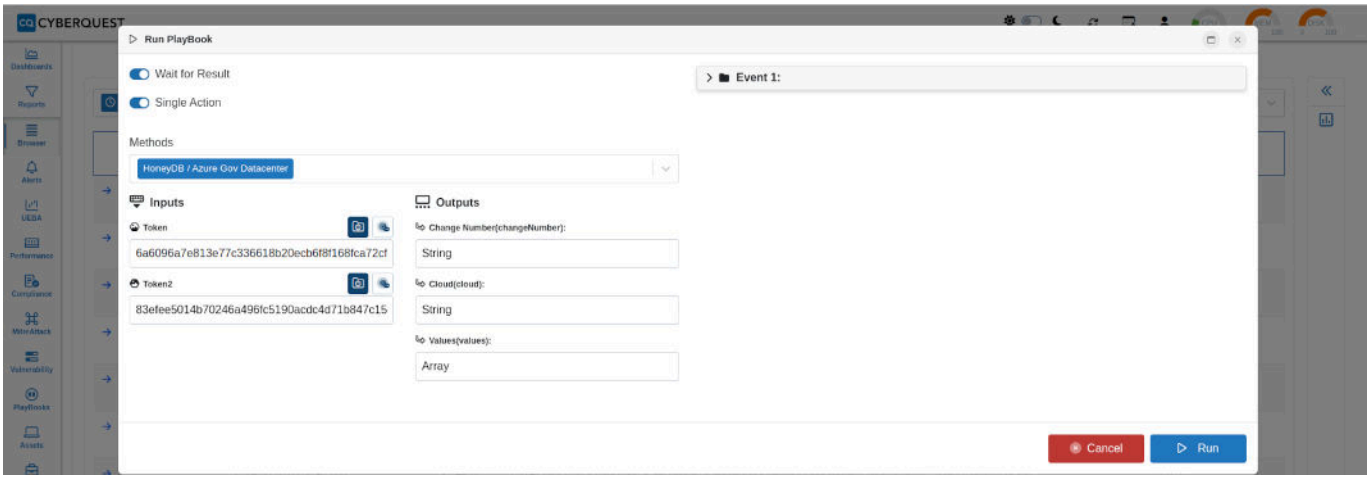


Inputs	Description
Token (is required)	The HoneyDB API ID is your identifier to use when querying HoneyDB APIs
Token2 (is required)	The threat information API key is required to query information from HoneyDB APIs

Outputs	Description
Created(created)	The timestamp when the datacenter was created
Prefixes(prefixes)	A list of IPs from that datacenter

HoneyDB/Oracle Datacenter method

Returns Oracle Cloud IP ranges.



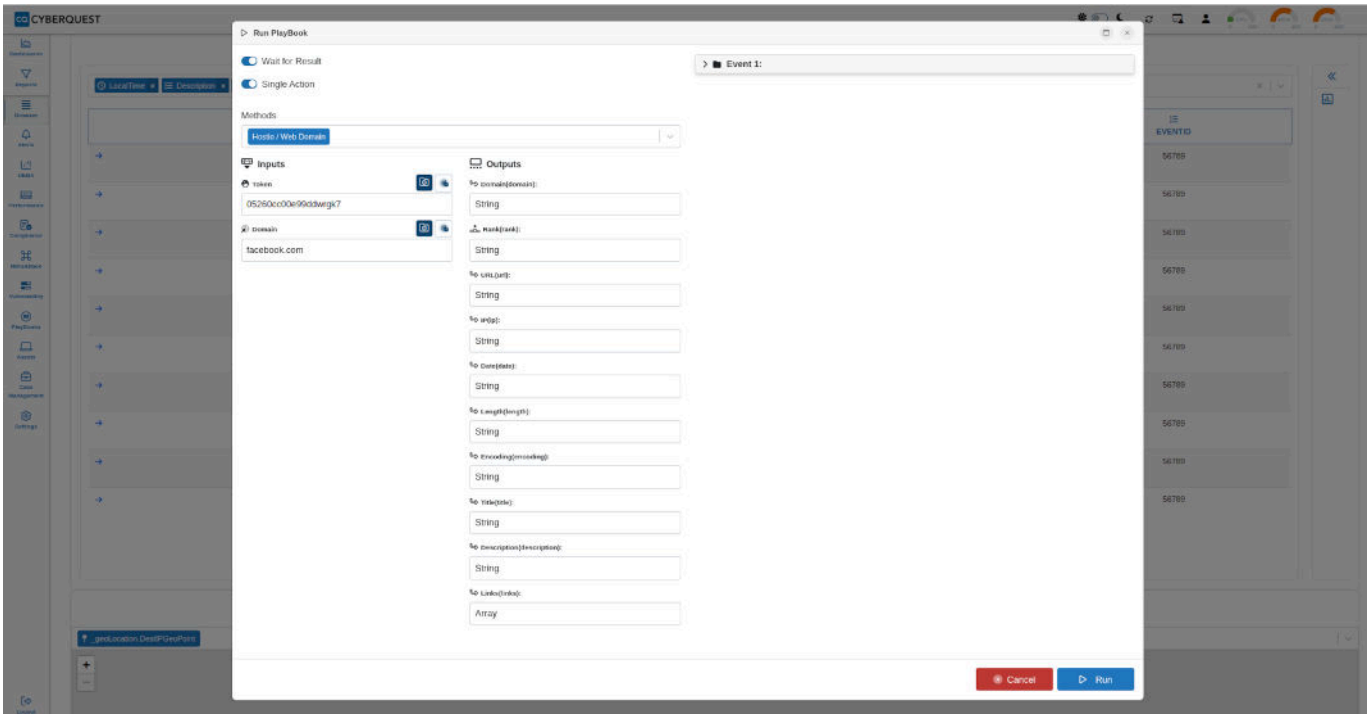
Inputs	Description
Token (is required)	The HoneyDB API ID is your identifier to use when querying HoneyDB APIs
Token2 (is required)	The threat information API key is required to query information from HoneyDB APIs

Outputs	Description
Lat Updated Timestamp(last_updated_timestamp) -> de modificat (LAST)	The timestamp when was last time updated
Regions(regions)	Details about dataceter

Host.io

Hostio/Web Domain method

Metadata scraped from a domain homepage.

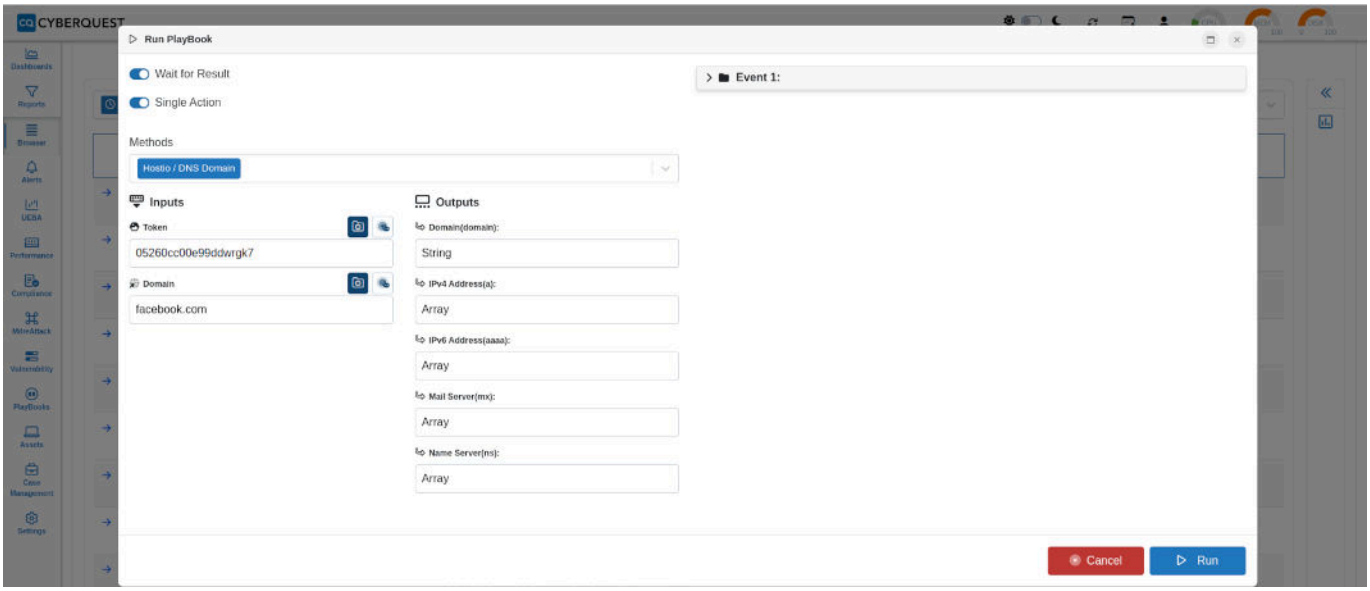


Inputs	Description
Token (is required)	To use the Host_io API, you must have an API key
Domain (is required)	The Domain that is being searched

Outputs	Description
Domain(domain)	The investigated domain
Rank(rank)	Position in host.io 10M domains ranking, https://host.io/rankings (https://host.io/rankings)
URL(url)	URL scraped from the data
IP(ip)	Actual IP scraped from the data
Date(date)	Date when the data was scraped
Length(length)	Length of the HTML content scraped
Encoding(encoding)	Encoding of the scraped data
Title(title)	HTML title
Description(description)	HTML meta description
Links(links)	Domains of links on the homepage

Hostio/DNS Domain method

Get all the DNS records stored for a domain.

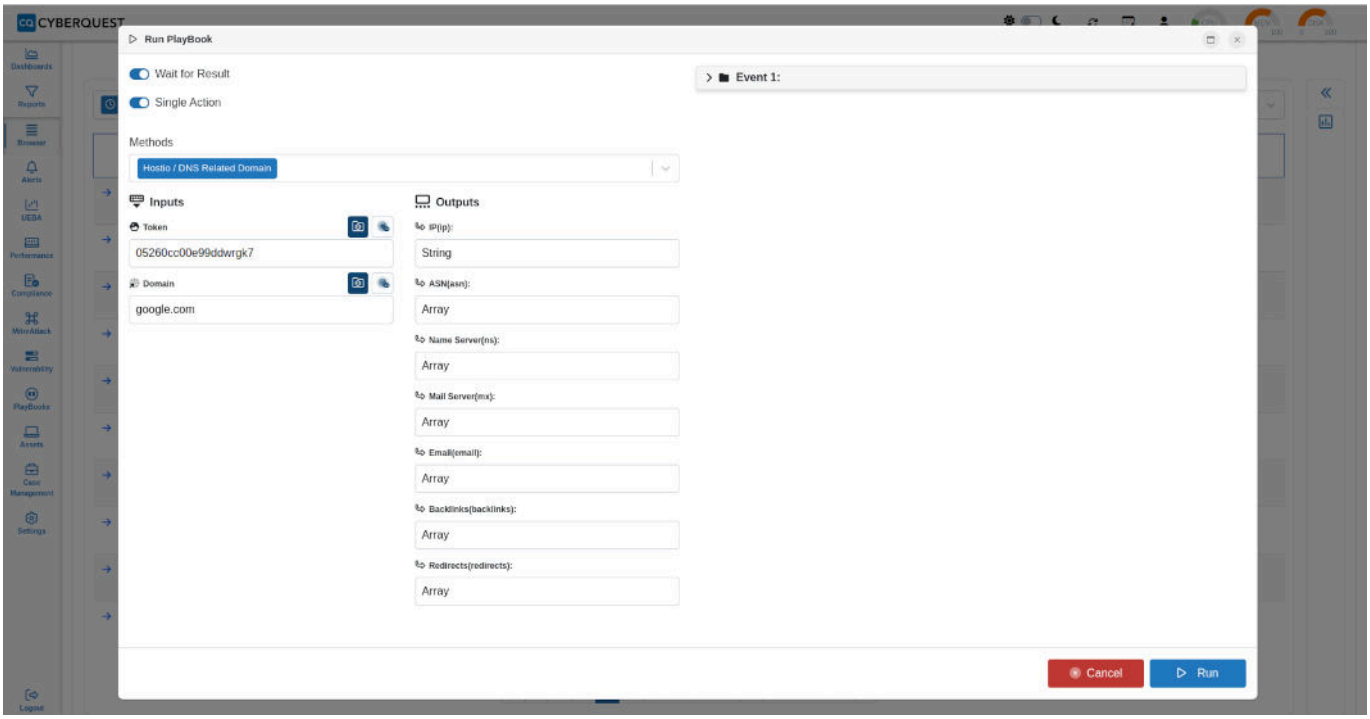


Inputs	Description
Token (is required)	To use the Host_io API, you must have an API key
Domain (is required)	The Domain that is being searched

Outputs	Description
Domain(domain)	The investigated domain
IPv4 Address(a)	A list of IPv4 addresses
IPv6 Address(aaaa)	A list of IPv6 addresses
Mail Server(mx)	A list of mail servers
Name Server(ns)	A list of name servers

Hostio/DNS Related Domain method

Get a count of the number of related domains for all supported lookups offered by Host.io.

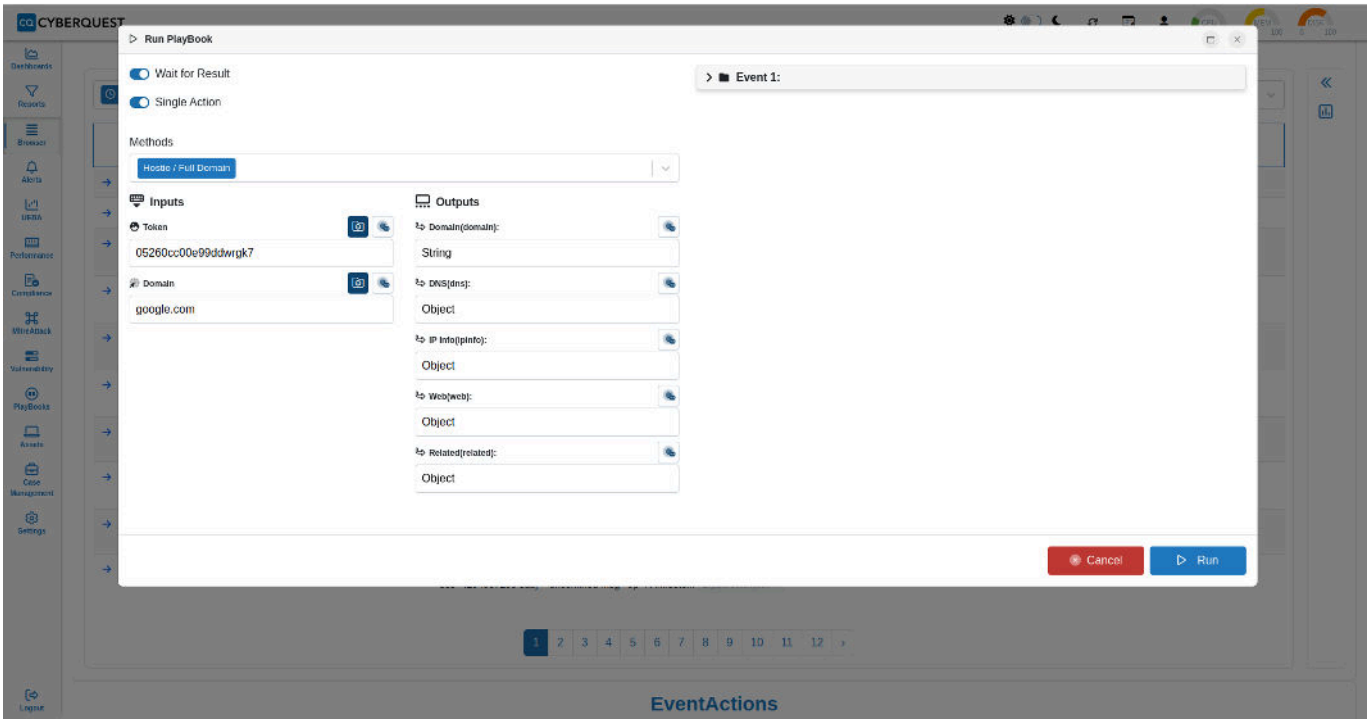


Inputs	Description
Token (is required)	To use the Host_io API, you must have an API key
Domain (is required)	The Domain that is being searched

Outputs	Description
IP(ip)	A list of related IPs
ASN(asn)	A list of ASN values
Name Server(ns)	A list of name servers
Mail Server(mx)	A list of mail servers
Email(email)	A list of emails
Backlinks(backlinks)	Domains that include a link to the domain on their homepage
Redirects(redirects)	Domains that redirect to the domain from their homepage

Hostio/Full Domain method

A single endpoint that includes the data from Web Domain, DNS Domain, Related Domain.

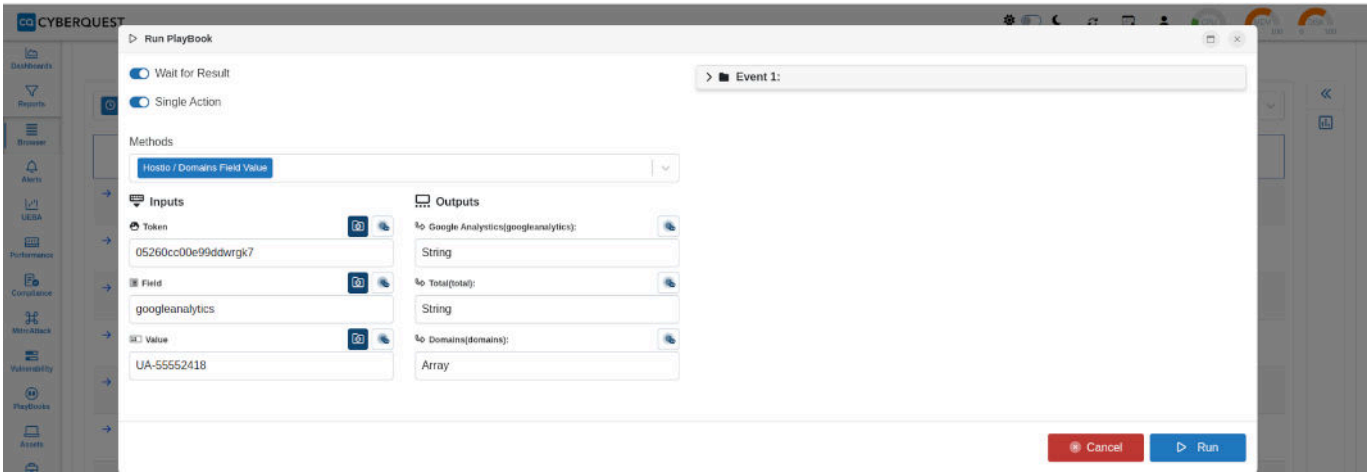


Inputs	Description
Token (is required)	To use the Host_io API, you must have an API key
Domain (is required)	The Domain that is being searched

Outputs	Description
Domain(domain)	The Domain that is being searched
DNS(dns)	DNS Details
IP Info(ipinfo)	IP info details
Web(web)	Web details
Related(related)	Related Details

Hostio/Domains Field Value method

Get all domains associated with field, and a count of the total. The value should be according to the field and not necessarily a domain.



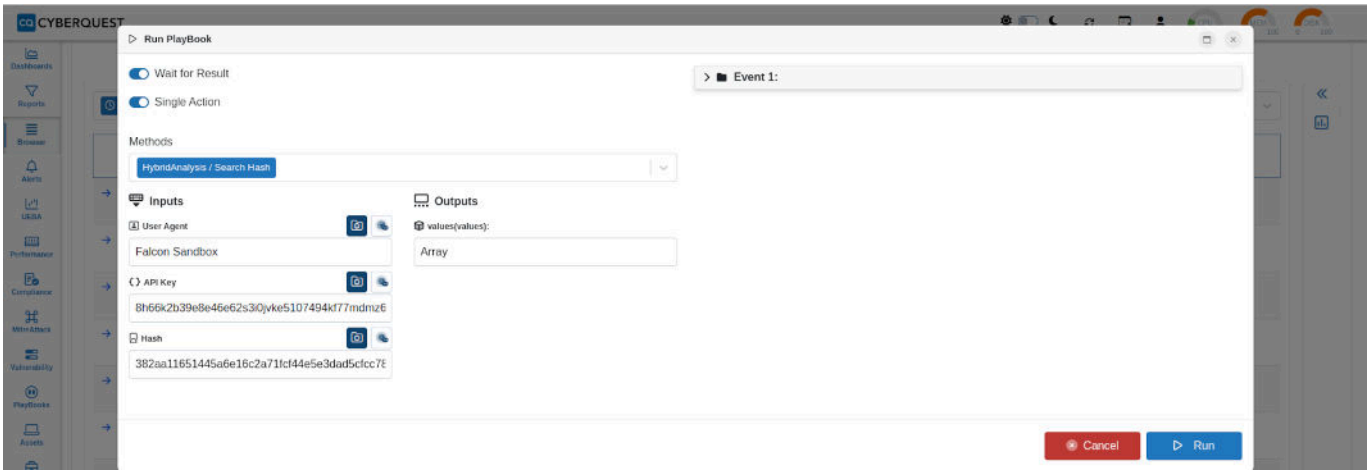
Inputs	Description
Token (is required)	To use the Host_io API, you must have an API key
Field (is required)	Domains associated with a field
Value (is required)	The value should be according to the field and not necessarily a domain

Outputs	Description
Google Analystics(googleanalytics)	Domains that include a googleanalytics ID on their homepage
Total(total)	The number of domains
Domains(domains)	A list of domains

HybridAnalysis

HybridAnalysis/Search Hash method

Summary for given hash.

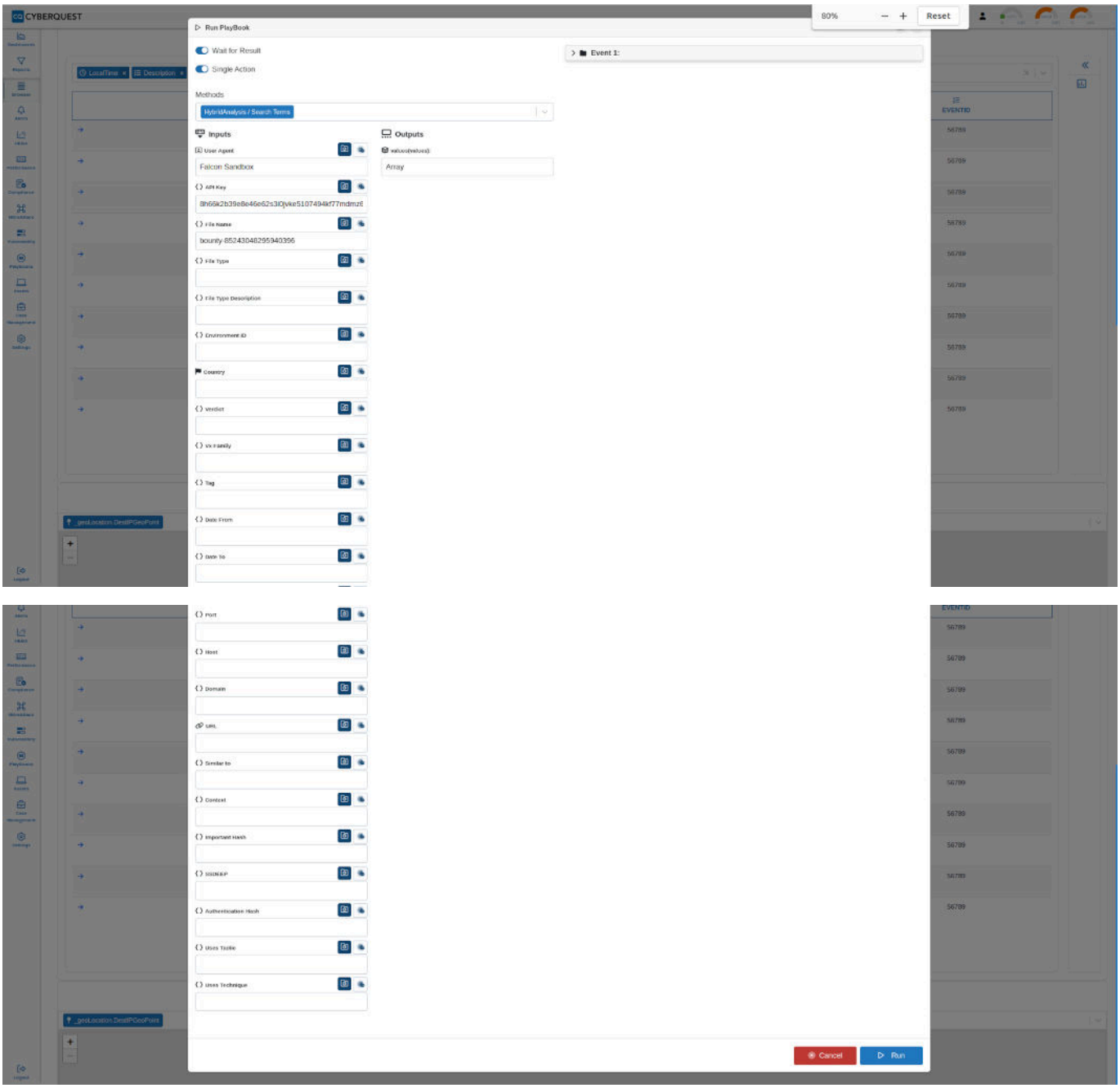


Inputs	Description
User Agent (is required)	Additionally, in order to bypass internal User-Agent blacklist checks, it is recommended to provide a typical User-Agent string or the product name Falcon
API Key (is required)	To use this API you must provide an API Key
Hash (is required)	MD5, SHA1 or SHA256

Outputs	Description
values(values)	The results of the API call

HybridAnalysis/Search Terms method

Search the database using the search terms.

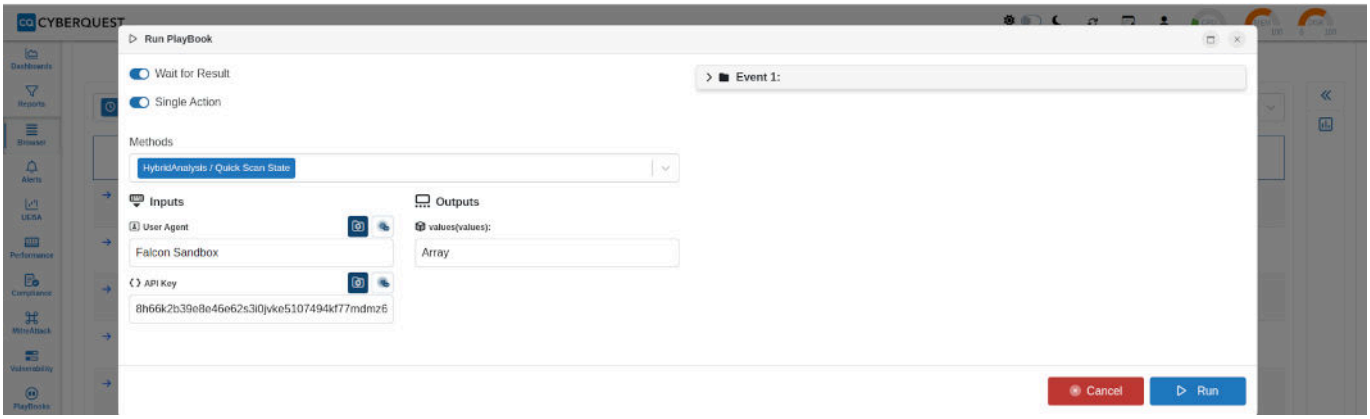

CYBERQUEST
Run PlayBook
Wait for Result
Single Action
Methods
HybridAnalysis / Search Terms
Inputs
Outputs
User Agent
Falcon Sandbox
API Key
File Name
bounty-8524304829594039 6
File Type
File Type Description
Environment ID
Country
Verdict
vx family
Tag
Date From
Date To
Array
Event 1:
80%
Reset
Port
Host
Domain
URL
Similar to
Context
Important Hash
SSDEEP
Authentication Hash
Uses Tactic
Uses Technique
Cancel
Run

Inputs	Description
User Agent (is required)	Additionally, in order to bypass internal User-Agent blacklist checks, it is recommended to provide a typical User-Agent string or the product name Falcon
API Key (is required)	To use this API you must provide an API Key
File Name	Filename e.g. invoice.exe
File Type	Filetype e.g. docx Available options: 64bits, android, assembly, bat, cmd, com, csv, data, doc, docker, docx, elf, empty, executable, flash, html, hwp, hwpx, img, iqy, java, javascript, library, lnk, macho, mshelp, msi, native, neexe, office, outlook, pdf, pedll, peexe, perl, ppt, pptx, ps, pub, python, rtf, script, sct, sh, svg, text, url, vbe, vbs, wsf, xls, xlsx
File Type Description	Filetype description e.g. PE32 executable
Environment ID	Environment Id
Country	Country (3 digit ISO) e.g. swe
Verdict	Verdict e.g. 1 Available options: 1 whitelisted, 2 no verdict, 3 no specific threat, 4 suspicious, 5 malicious
Vx Family	AV Family Substring e.g. nemucod
Tag	Hashtag e.g. ransomware
Date From	Date from in format: Y-m-d H:i e.g. 2018-09-28 15:30
Date To	Date to in format: Y-m-d H:i e.g. 2018-09-28 15:30
Port	Port e.g. 8080
Host	Host e.g. 192.168.0.1
Domain	Domain e.g. checkip.dyndns.org
URL	HTTP Request Substring e.g. google
Similar to	
Context	
Important Hash	Unique value for a file based on the libraries and functions that it imports. It is useful for identifying and categorizing malware samples
SSDEEP	Technique for comparing files based on their similarity, not their exact content. It uses a special hash function that divides the file into segments and calculates a value for each segment
Authentication Hash	Authentication hash is a feature of hybrid analysis that allows users to search for malware samples based on their cryptographic hash values
Uses Tactic	Uses MITRE ATT&CK® Tactic. Please check they website to get current Tactics
Uses Technique	Uses MITRE ATT&CK® Technique. Please check they website to get current Techniques

Outputs	Description
values(values)	The results of the API call

HybridAnalysis/Quick Scan State method

Return list of available scanners.

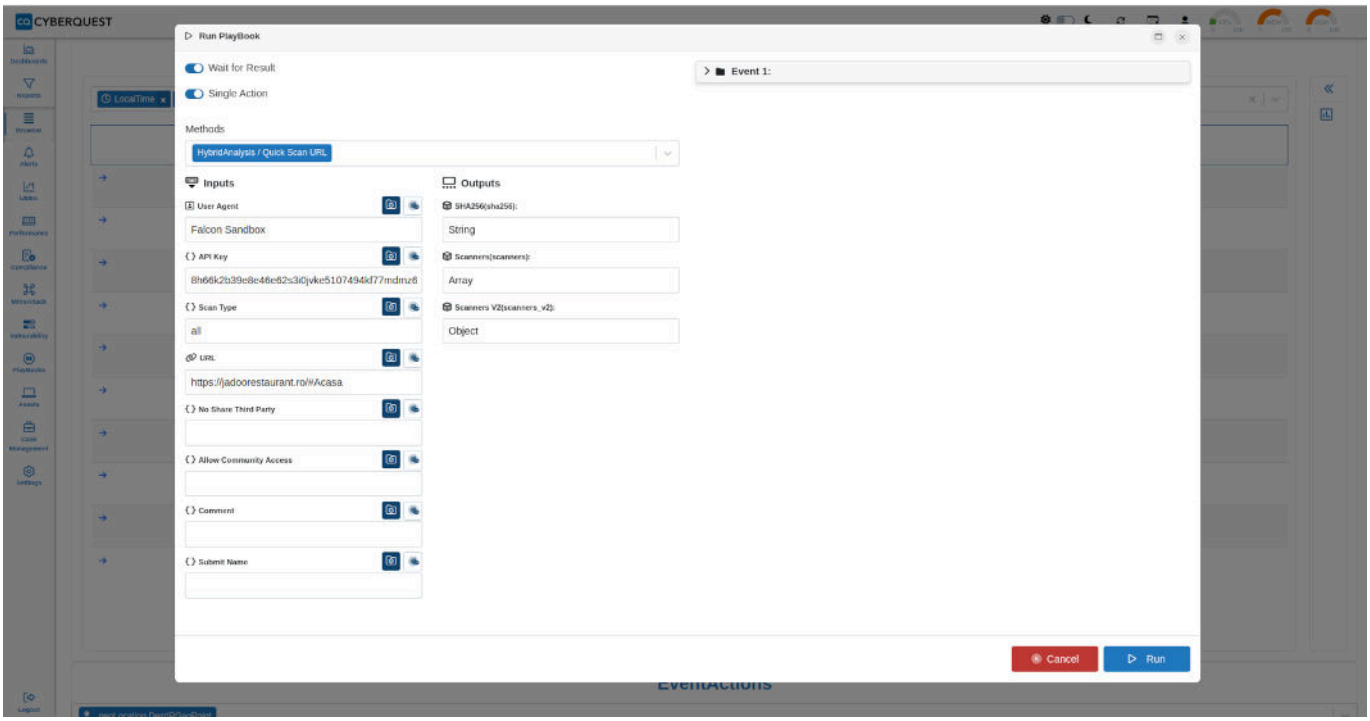


Inputs	Description
User Agent (is required)	Additionally, in order to bypass internal User-Agent blacklist checks, it is recommended to provide a typical User-Agent string or the product name Falcon
API Key (is required)	To use this API you must provide an API Key

Outputs	Description
values(values)	The results the API call

HybridAnalysis/Quick Scan URL method

Submit a websites url or url with file for analysis.

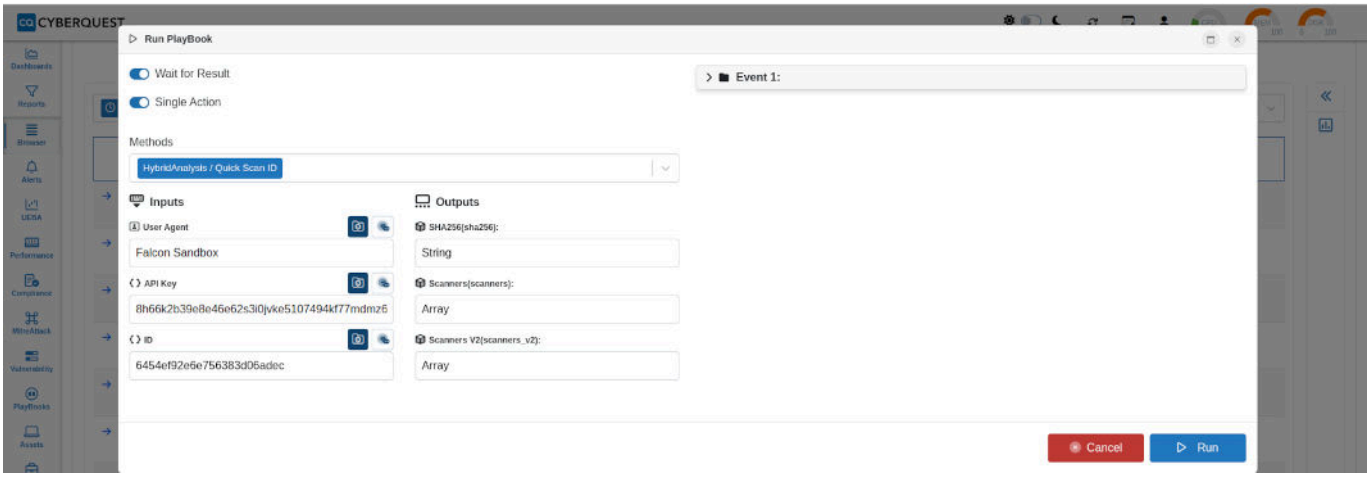


Inputs	Description
User Agent (is required)	Additionally, in order to bypass internal User-Agent blacklist checks, it is recommended to provide a typical User-Agent string or the product name Falcon
API Key (is required)	To use this API you must provide an API Key
Scan Type (is required)	Type of scan, please see /quick-scan/state to see available scanners
URL (is required)	Websites url or url with file to submit
No Share Third Party	When set to true, the sample is never shared with any third party. Default: true
Allow Community Access	When set to true, the sample will be available for the community. Default: true (Note: when no_share_third_party is set to false, it wont be possible to set different value than true)
Comment	Optional comment text that may be associated with the submission/sample (Note: you can use #tags here)
Submit Name	Optional submission name field that will be used for file type detection and analysis

Outputs	Description
SHA256(sha256)	The investigated SHA
Scanners(scanners)	The scanners used in analysis
Scanners V2(scanners_v2)	The scanners used in analysis

HybridAnalysis/Quick Scan ID method

Some scanners need time to process file, if in response finished is set to false, then you need use this endpoint to get final results.

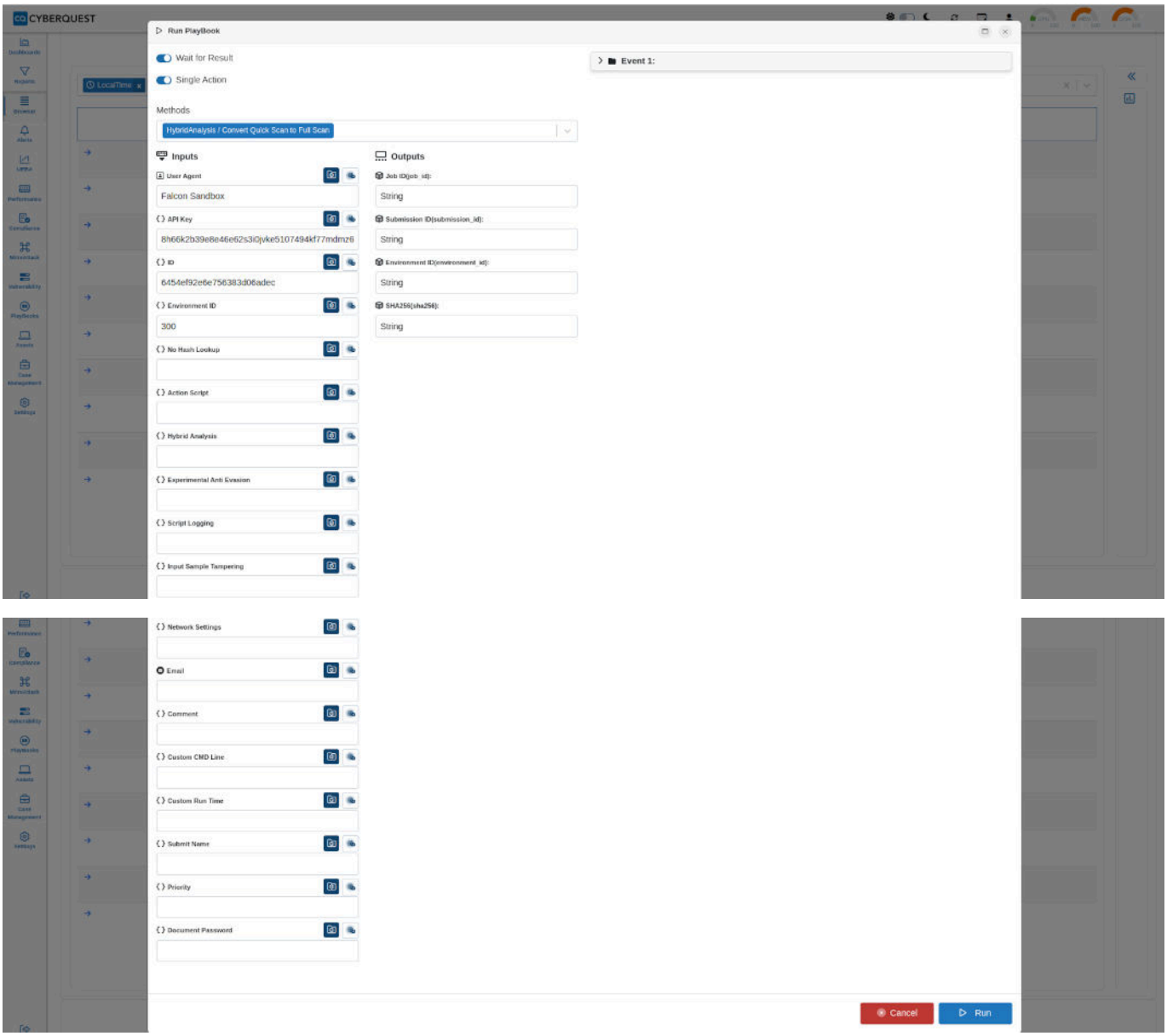


Inputs	Description
User Agent (is required)	Additionally, in order to bypass internal User-Agent blacklist checks, it is recommended to provide a typical User-Agent string or the product name Falcon
API Key (is required)	To use this API you must provide an API Key
ID	ID of scan

Outputs	Description
SHA256(sha256)	The investigated SHA
Scanners(scanners)	The scanners used in analysis
Scanners V2(scanners_v2)	The scanners used in analysis

HybridAnalysis/Convert Quick Scan to Full Scan method

Convert quick scan to sandbox report.

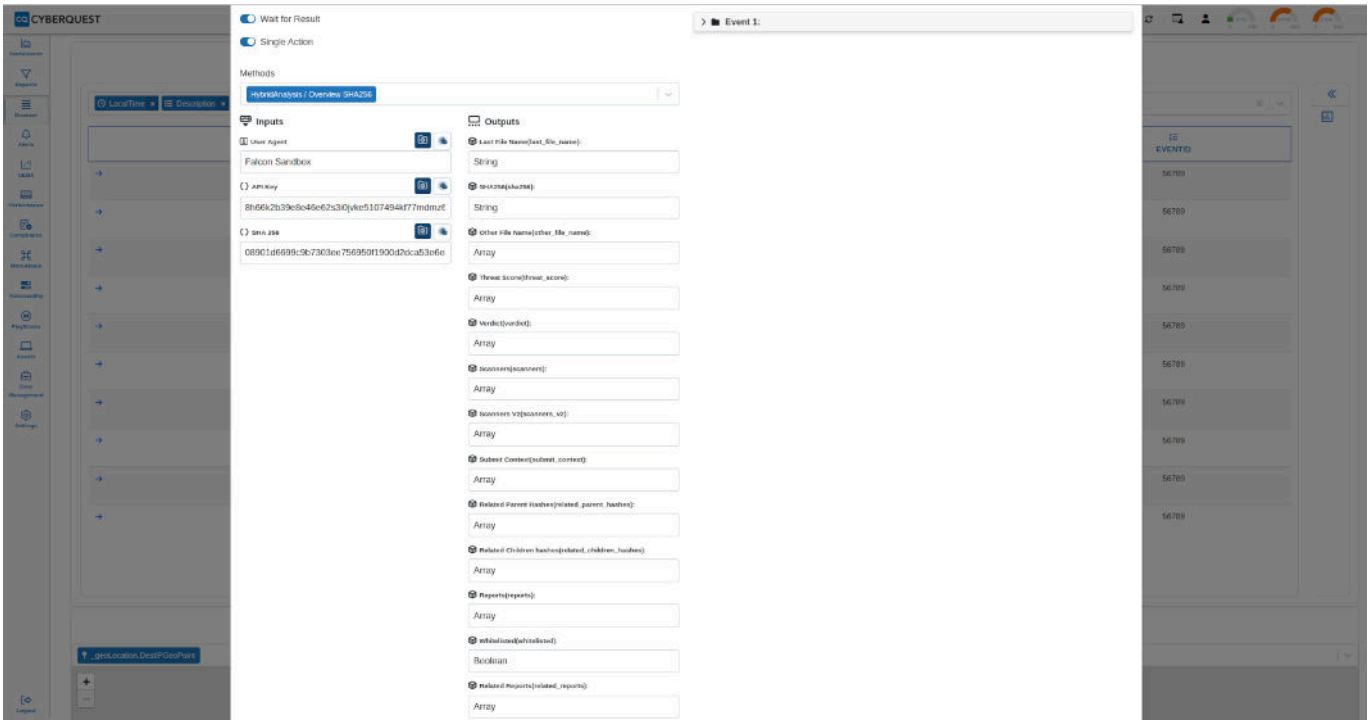


Inputs	Description
User Agent (is required)	Additionally, in order to bypass internal User-Agent blacklist checks, it is recommended to provide a typical User-Agent string or the product name Falcon
API Key (is required)	To use this API you must provide an API Key
ID (is required)	ID of quick scan to convert
Environment ID (is required)	Environment ID. Available environments ID: 400: Mac Catalina 64 bit (x86), 310: Linux (Ubuntu 20.04, 64 bit), 300: Linux (Ubuntu 16.04, 64 bit), 200: Android Static Analysis, 160: Windows 10 64 bit, 120: Windows 7 64 bit, 110: Windows 7 32 bit (HWP Support), 100: Windows 7 32 bit
No Hash Lookup	Default: false
Action Script	Optional custom runtime action script. Available runtime scripts: default, default_maxantievasion, default_randomfiles, default_randomtheme, default_openie
Hybrid Analysis	When set to false, no memory dumps or memory dump analysis will take place. Default: true
Experimental Anti Evasion	When set to true, will set all experimental anti-evasion options of the Kernelmode Monitor. Default: false
Script Logging	When set to true, will set the in-depth script logging engine of the Kernelmode Monitor. Default: false
Input Sample Tampering	When set to true, will allow experimental anti-evasion options of the Kernelmode Monitor that tamper with the input sample. Default: false
Network Settings	Network settings, by the default, fully operating network is set. Available options: default: Fully operating network, tor: Route network traffic via TOR, simulated: Simulate network traffic
Email	Optional E-Mail address that may be associated with the submission for notification
Comment	Optional comment text that may be associated with the submission/sample (Note: you can use #tags here)
Custom CMD Line	Optional commandline that should be passed to the analysis file
Custom Run Time	Optional runtime duration (in seconds)
Submit Name	Optional submission name field that will be used for file type detection and analysis
Priority	Optional priority value between 1 (lowest) and 10 (highest), by default all samples run with highest priority
Document Password	Optional document password that will be used to fill-in Adobe/Office password prompts

Outputs	Description
Job ID(job_id)	The job ID
Submission ID(submission_id)	The submission ID of the request
Environment ID(environment_id)	The environment ID
SHA256(sha256)	The SHA generated for this scan

HybridAnalysis/Overview SHA256 method

Return overview for hash.

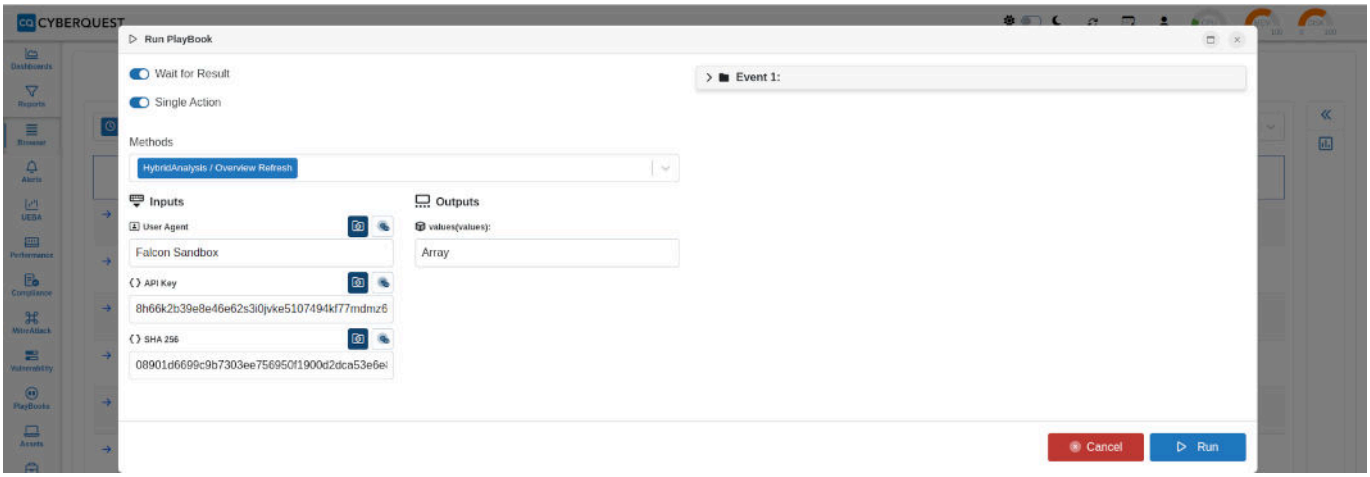


Inputs	Description
User Agent (is required)	Additionally, in order to bypass internal User-Agent blacklist checks, it is recommended to provide a typical User-Agent string or the product name Falcon
API Key (is required)	To use this API you must provide an API Key
SHA 256 (is required)	SHA256 for lookup

Outputs	Description
Last File Name(last_file_name)	The last known name
SHA256(sha256)	The investigated SHA
Other File Name(other_file_name)	Possible other name of the file
Threat Score(threat_score)	The threat score calculated by HybridAnalysis
Verdict(verdict)	Verdict e.g. 1 Available options: 1 whitelisted, 2 no verdict, 3 no specific threat, 4 suspicious, 5 malicious
Scanners(scanners)	The scanners used in analysis
Scanners V2(scanners_v2)	The scanners used in analysis
Submit Context(submit_context)	Details about submission of investigation
Related Parent Hashes(related_parent_hashes)	A list of parent related hashes
Related Children hashes(related_children_hashes)	A list of children related hashes
Reports(reports)	A list of reports for the investigated hash
Whitelisted(whitelisted)	True if the SHA is whitelisted
Related Reports(related_reports)	A list of reports related

HybridAnalysis/Overview Refresh method

Refresh overview and download fresh data from external services.

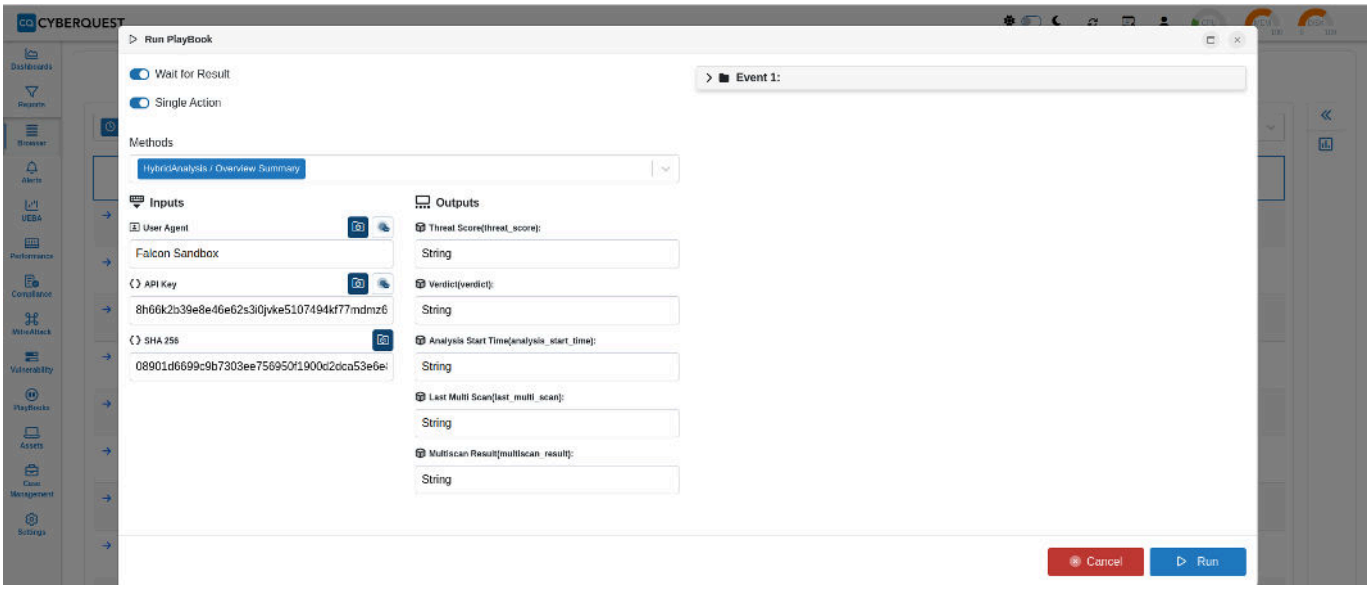


Inputs	Description
User Agent (is required)	Additionally, in order to bypass internal User-Agent blacklist checks, it is recommended to provide a typical User-Agent string or the product name Falcon
API Key (is required)	To use this API you must provide an API Key
SHA 256 (is required)	SHA256 for lookup

Outputs	Description
values(values)	The results of the API call

HybridAnalysis/Overview Summary method

Return overview for hash.

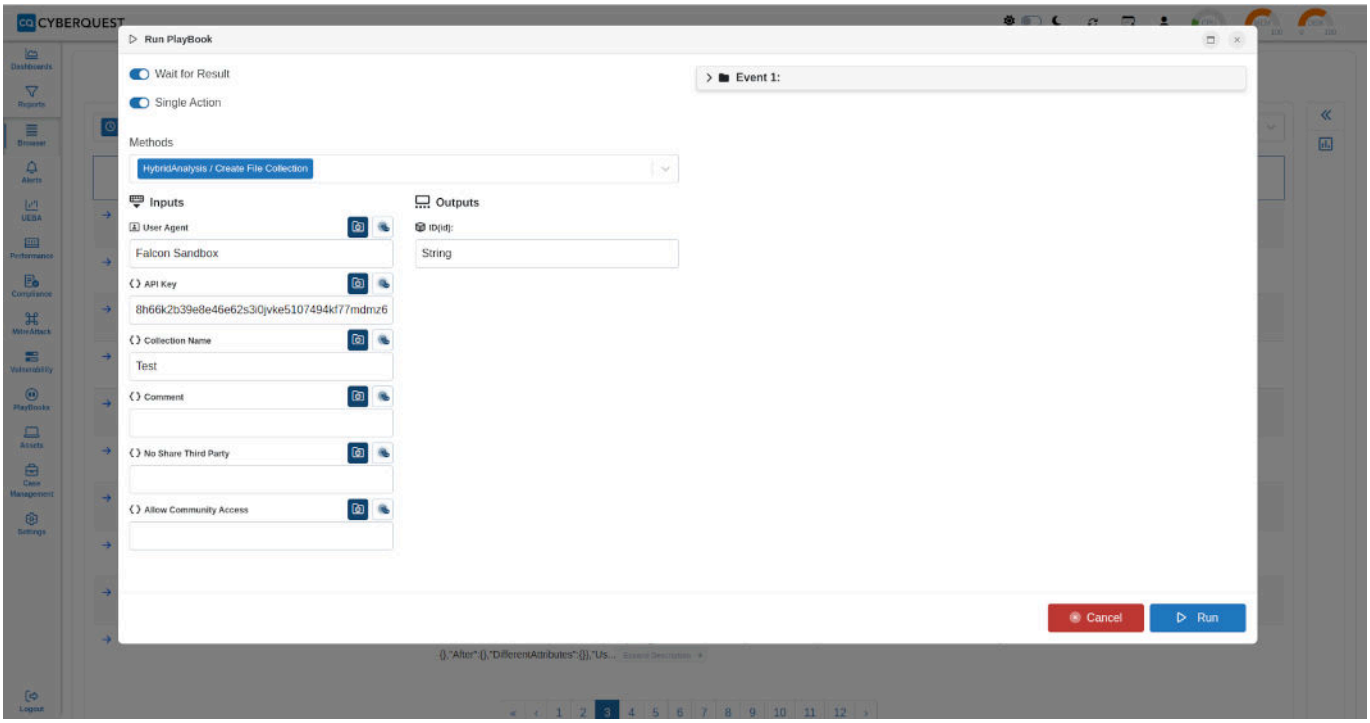


Inputs	Description
User Agent (is required)	Additionally, in order to bypass internal User-Agent blacklist checks, it is recommended to provide a typical User-Agent string or the product name Falcon
API Key (is required)	To use this API you must provide an API Key
SHA 256 (is required)	SHA256 for lookup

Outputs	Description
Threat Score(threat_score)	The threat score calculated by HybridAnalysis
Verdict(verdict)	Verdict e.g. 1 Available options: 1 whitelisted, 2 no verdict, 3 no specific threat, 4 suspicious, 5 malicious
Analysis Start Time(analysis_start_time)	The timestamp when the analysis start
Last Multi Scan(last_multi_scan)	The timestamp of tha last multi scan
Multiscan Result(multiscan_result)	The number of results from multi scan

HybridAnalysis/Create File Collection method

Create file collection.

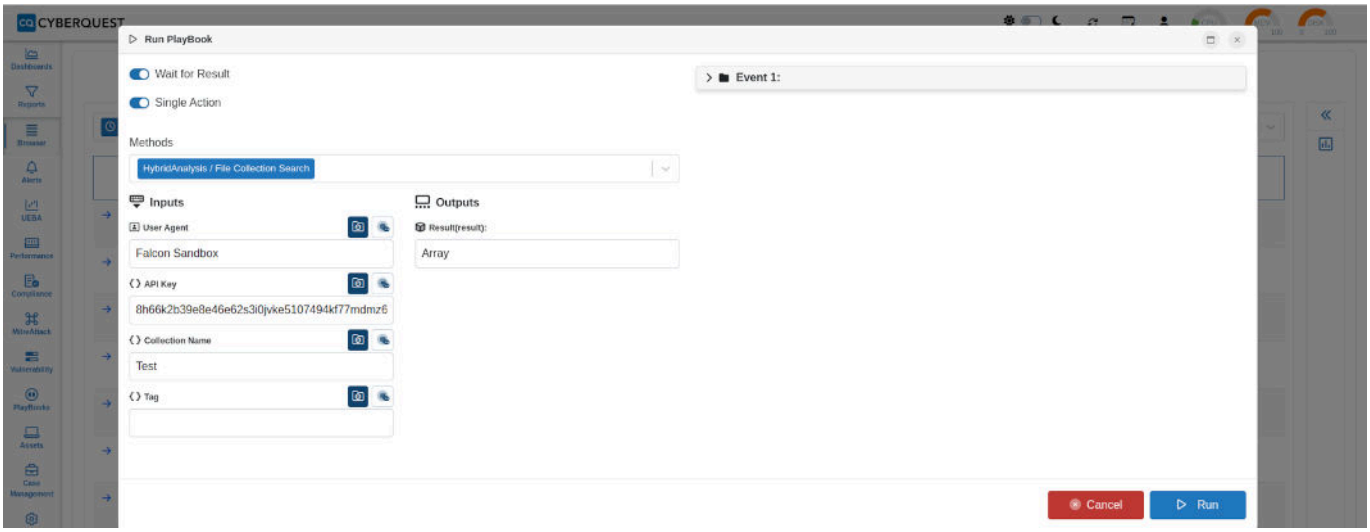


Inputs	Description
User Agent (is required)	Additionally, in order to bypass internal User-Agent blacklist checks, it is recommended to provide a typical User-Agent string or the product name Falcon
API Key (is required)	To use this API you must provide an API Key
Collection Name	Optional collection name
Comment	Optional comment text that may be associated with the file collection (Note: you can use #tags here)
No Share Third Party	When set to true, samples within collection will never be shared with any third party. Default: true
Allow Community Access	When set to true, samples within collection will be available for the community. Default: true

Outputs	Description
ID(id)	The ID of the new Collection Created

HybridAnalysis/File Collection Search method

Search the database using the search terms.

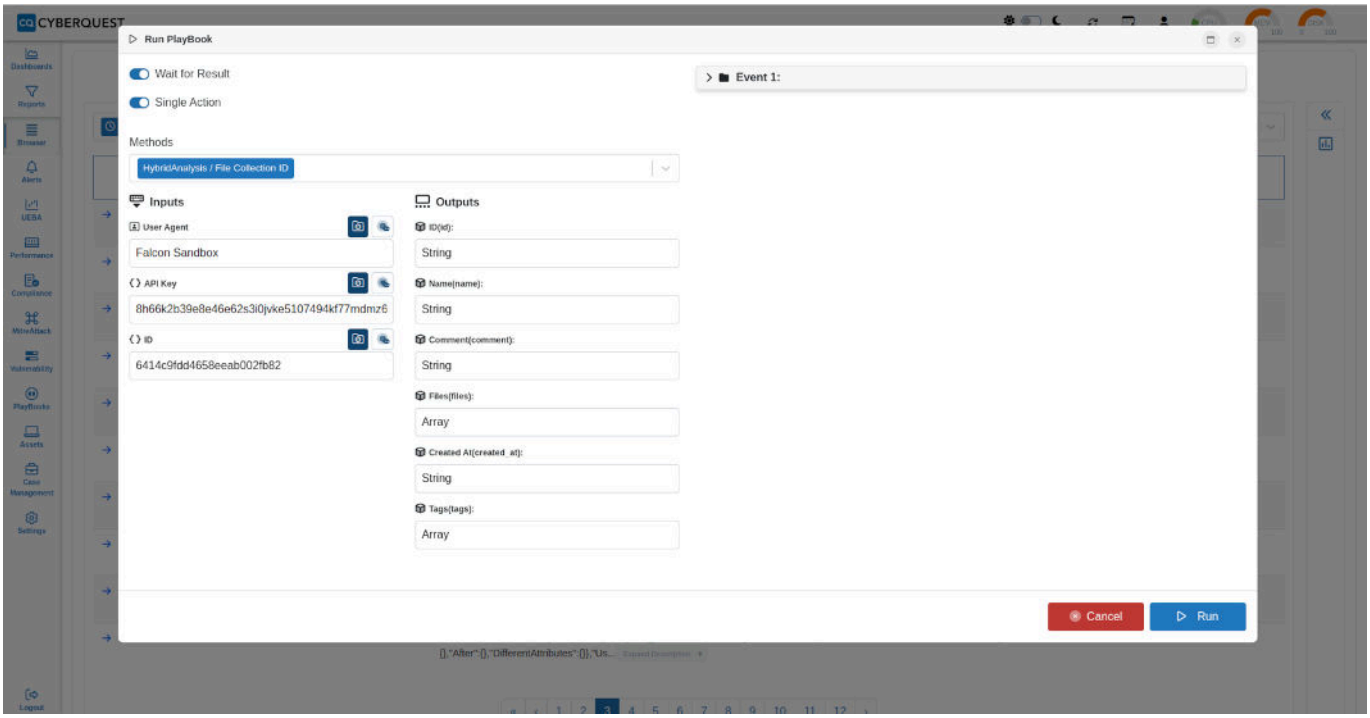


Inputs	Description
User Agent (is required)	Additionally, in order to bypass internal User-Agent blacklist checks, it is recommended to provide a typical User-Agent string or the product name Falcon
API Key (is required)	To use this API you must provide an API Key
Collection Name	Collection Name
Tag	Hashtag e.g. ransomware

Outputs	Description
Result(result)	The results of the API call

HybridAnalysis/File Collection ID method

Return a summary of file collection.

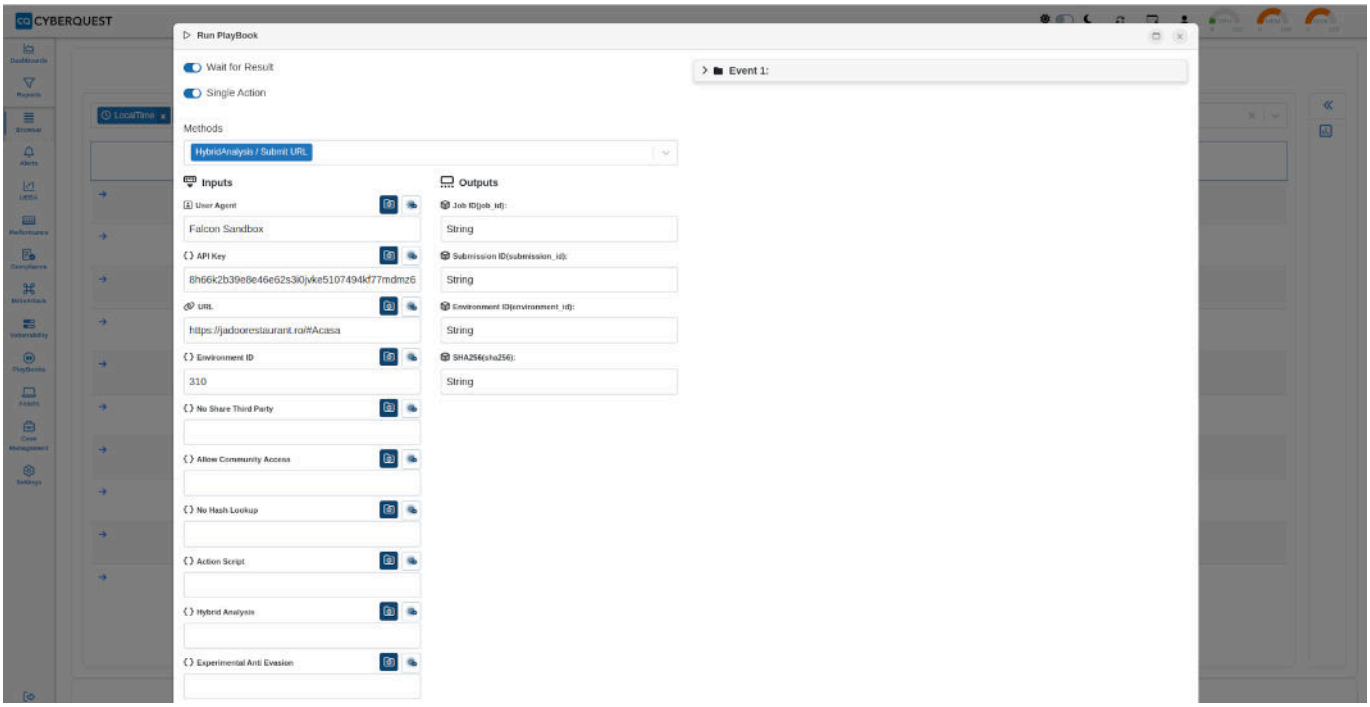


Inputs	Description
User Agent (is required)	Additionally, in order to bypass internal User-Agent blacklist checks, it is recommended to provide a typical User-Agent string or the product name Falcon
API Key (is required)	To use this API you must provide an API Key
ID (is required)	File collection id

Outputs	Description
ID(id)	File collection id
Name(name)	The name of collection
Comment(comment)	Details about collection
Files(files)	A list of files from this collection
Created At(created_at)	The timestamp when the collection was created
Tags(tags)	A list of possible tags assigned to the collection

HybridAnalysis/Submit URL method

Submit a websites url or url with file for analysis.



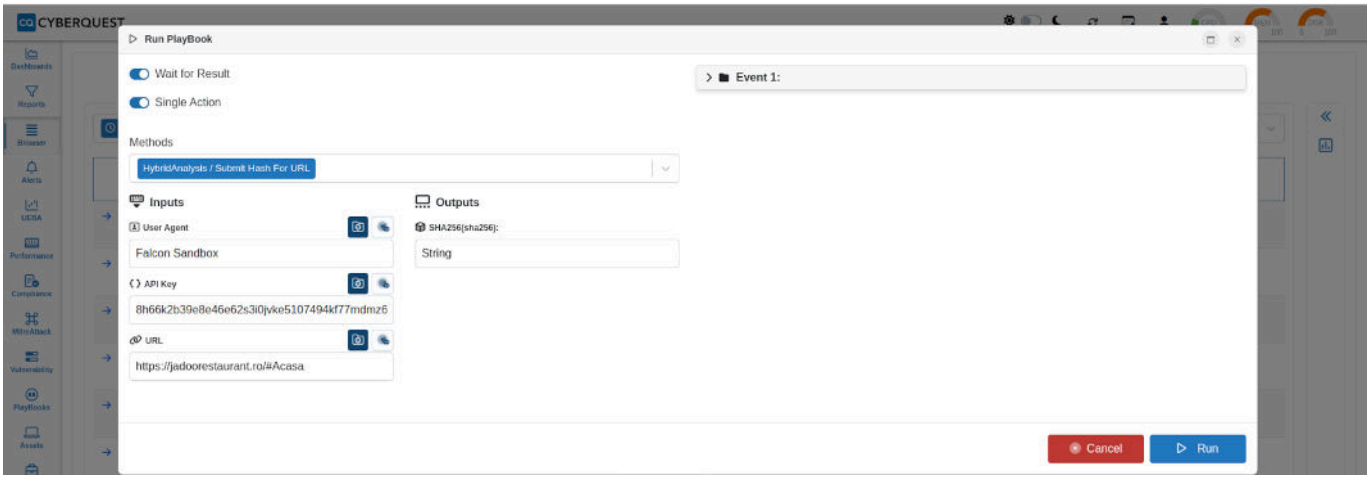

CYBERQUEST
Script Logging
Input Sample Tempering
Network Settings
Email
Comment
Custom Date Time
Cstom CMD Line
Custom Run Time
Submit Name
Priority
Document Password
Environment Variable
Cancel
Run

Inputs	Description
User Agent (is required)	Additionally, in order to bypass internal User-Agent blacklist checks, it is recommended to provide a typical User-Agent string or the product name Falcon
API Key (is required)	To use this API you must provide an API Key
URL (is required)	URL for analyze or url of file to submit
Environment ID (is required)	Environment ID. Available environments ID: 400: Mac Catalina 64 bit (x86), 310: Linux (Ubuntu 20.04, 64 bit), 300: Linux (Ubuntu 16.04, 64 bit), 200: Android Static Analysis, 160: Windows 10 64 bit, 120: Windows 7 64 bit, 110: Windows 7 32 bit (HWP Support), 100: Windows 7 32 bit
No Share Third Party	When set to true, the sample is never shared with any third party. Default: true
Allow Community Access	When set to true, the sample will be available for the community. Ignored unless url contains a file, in other case, there will be a true value. Default: true
No Hash Lookup	Default: false
Action Script	Optional custom runtime action script. Available runtime scripts: default, default_maxantievasion, default_randomfiles, default_randomtheme, default_openie
Hybrid Analysis	When set to false, no memory dumps or memory dump analysis will take place. Default: true
Experimental Anti Evasion	When set to true, will set all experimental anti-evasion options of the Kernelmode Monitor. Default: false
Script Logging	When set to true, will set the in-depth script logging engine of the Kernelmode Monitor. Default: false
Input Sample Tempering	When set to true, will allow experimental anti-evasion options of the Kernelmode Monitor that tamper with the input sample. Default: false
Network Settings	Network settings, by the default, fully operating network is set. Available options: default: Fully operating network, tor: Route network traffic via TOR, simulated: Simulate network traffic
Email	Optional E-Mail address that may be associated with the submission for notification
Comment	Optional comment text that may be associated with the submission/sample (Note: you can use #tags here)
Custom Date Time	Optional custom date/time that can be set for the analysis system. Expected format: yyyy-MM-dd HH:mm
Cstom CMD Line	Optional commandline that should be passed to the analysis file
Custom Run Time	Optional runtime duration (in seconds)
Submit Name	Optional submission name field that will be used for file type detection and analysis. Ignored unless url contains a file
Priority	Optional priority value between 1 (lowest) and 10 (highest), by default all samples run with highest priority
Document Password	Optional document password that will be used to fill-in Adobe/Office password prompts. Ignored unless url contains a file
Environment Variable	Optional system environment value. The value is provided in the format: name: value

Outputs	Description
Job ID(job_id)	The job ID
Submission ID(submission_id)	The submission ID of the request
Environment ID(environment_id)	The environment ID
SHA256(sha256)	The SHA generated for this scan

HybridAnalysis/Submit Hash For URL method

Determine a SHA256 that an online file or URL submission will have when being processed by the system. Note: this is useful when looking up URL analysis.

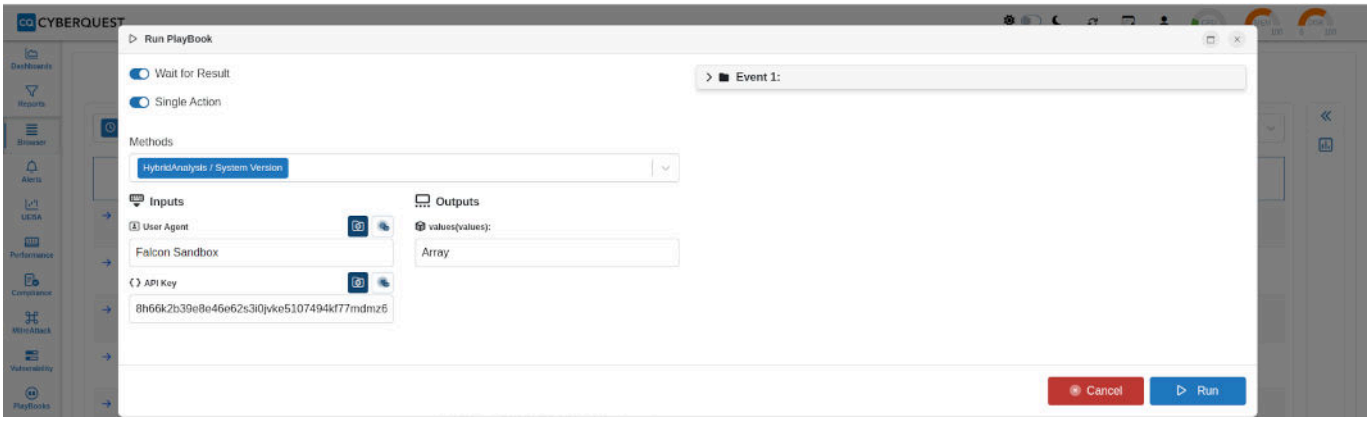


Inputs	Description
User Agent (is required)	Additionally, in order to bypass internal User-Agent blacklist checks, it is recommended to provide a typical User-Agent string or the product name Falcon
API Key (is required)	To use this API you must provide an API Key
URL (is required)	Url to check

Outputs	Description
SHA256(sha256)	The SHA generated for URL checked

HybridAnalysis/System Version method

Return system elements versions.

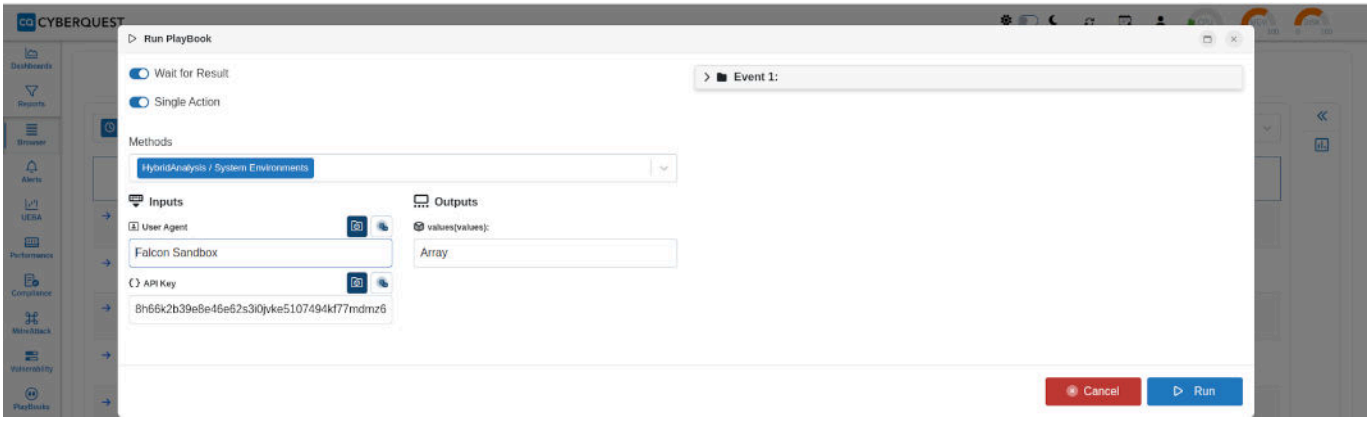


Inputs	Description
User Agent (is required)	Additionally, in order to bypass internal User-Agent blacklist checks, it is recommended to provide a typical User-Agent string or the product name Falcon
API Key (is required)	To use this API you must provide an API Key

Outputs	Description
values(values)	The results of the API call

HybridAnalysis/System Environments method

Return information about available execution environments.

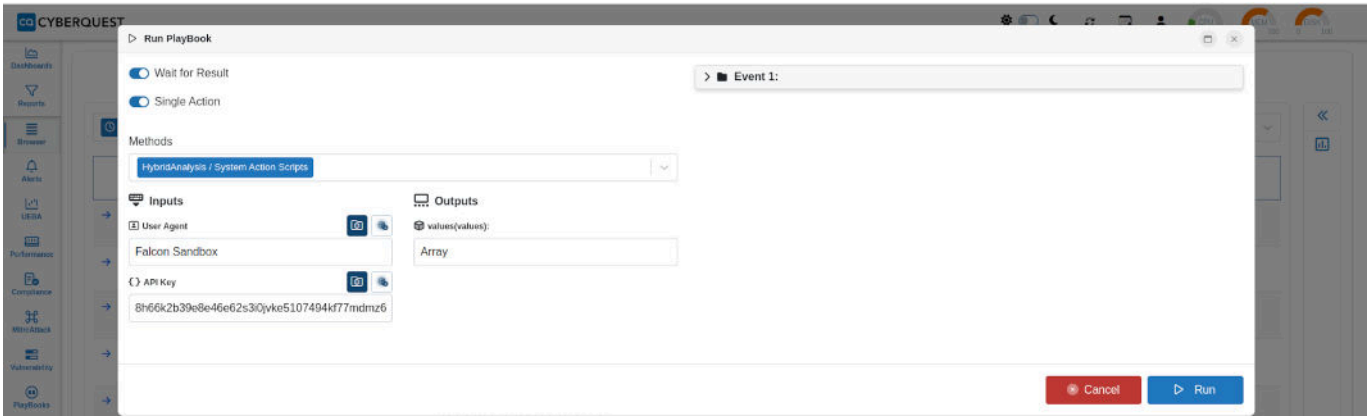


Inputs	Description
User Agent (is required)	Additionally, in order to bypass internal User-Agent blacklist checks, it is recommended to provide a typical User-Agent string or the product name Falcon
API Key (is required)	To use this API you must provide an API Key

Outputs	Description
values(values)	The results of the API call

HybridAnalysis/System Action Scripts method

Return information about available action scripts.

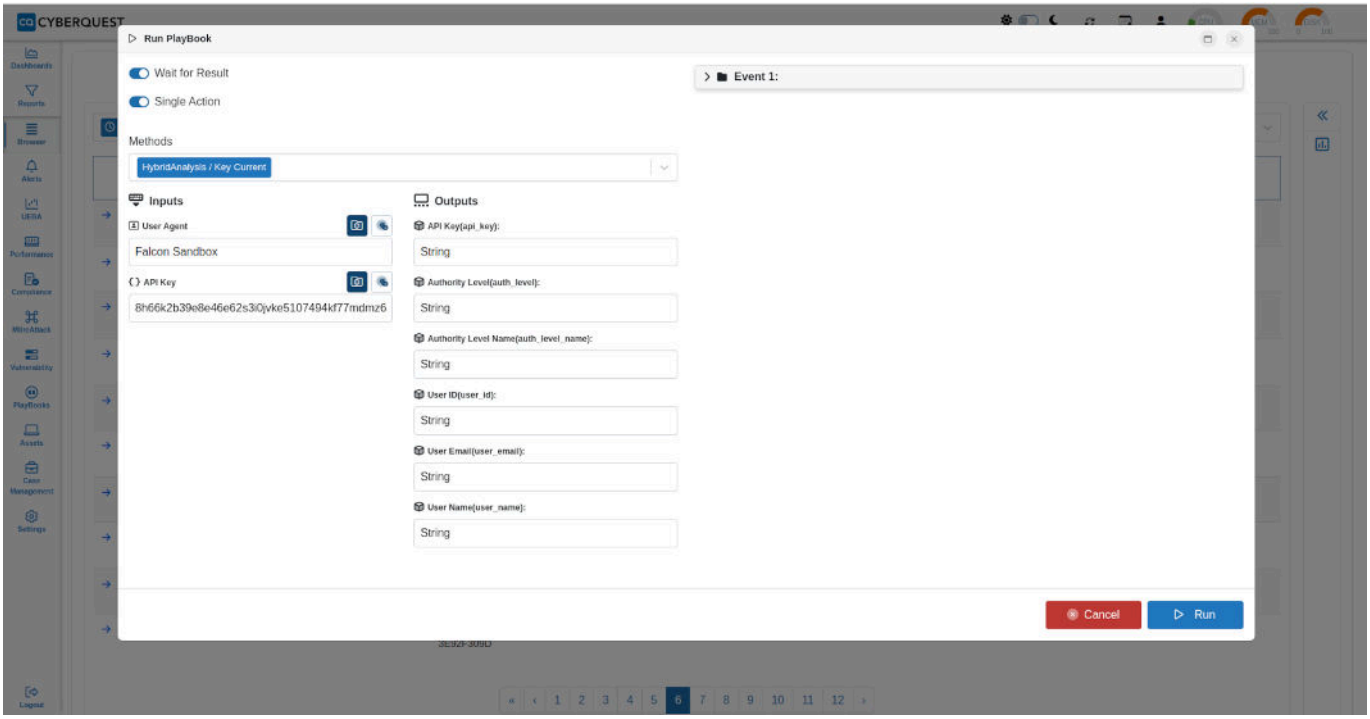


Inputs	Description
User Agent (is required)	Additionally, in order to bypass internal User-Agent blacklist checks, it is recommended to provide a typical User-Agent string or the product name Falcon
API Key (is required)	To use this API you must provide an API Key

Outputs	Description
values(values)	The results of the API call

HybridAnalysis/Key Current method

Return information about the used API key and it limits.

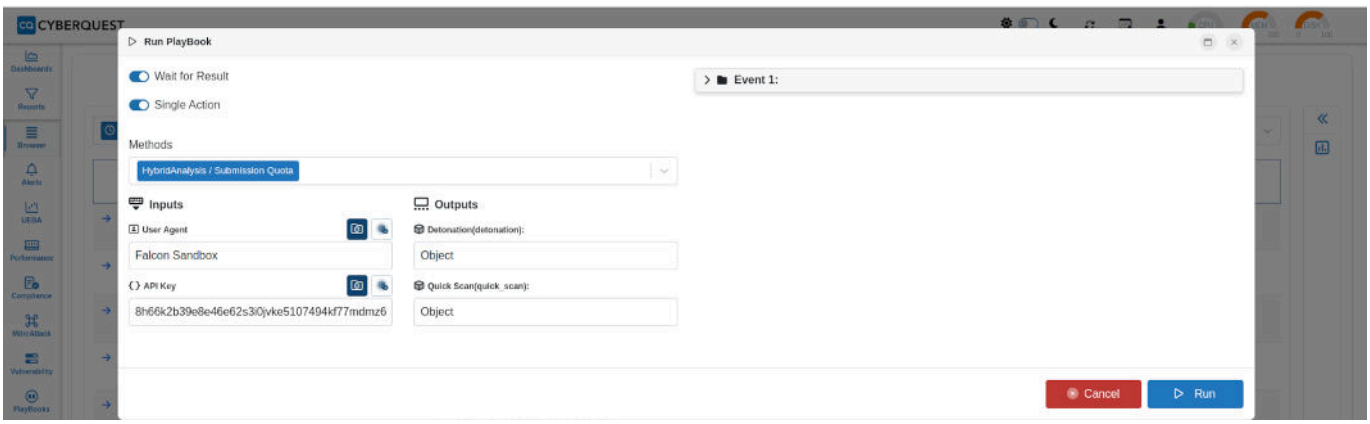


Inputs	Description
User Agent (is required)	Additionally, in order to bypass internal User-Agent blacklist checks, it is recommended to provide a typical User-Agent string or the product name Falcon
API Key (is required)	To use this API you must provide an API Key

Outputs	Description
API Key(api_key)	The API key used for this API call
Authority Level(auth_level)	Authority level of the API key
Authority Level Name(auth_level_name)	Authority name level of the API key
User ID(user_id)	The user ID which has the API key associated
User Email(user_email)	The user email which has the API key associated
User Name(user_name)	The user name which has the API key associated

HybridAnalysis/Submission Quota method

Return information about quota and current usage.

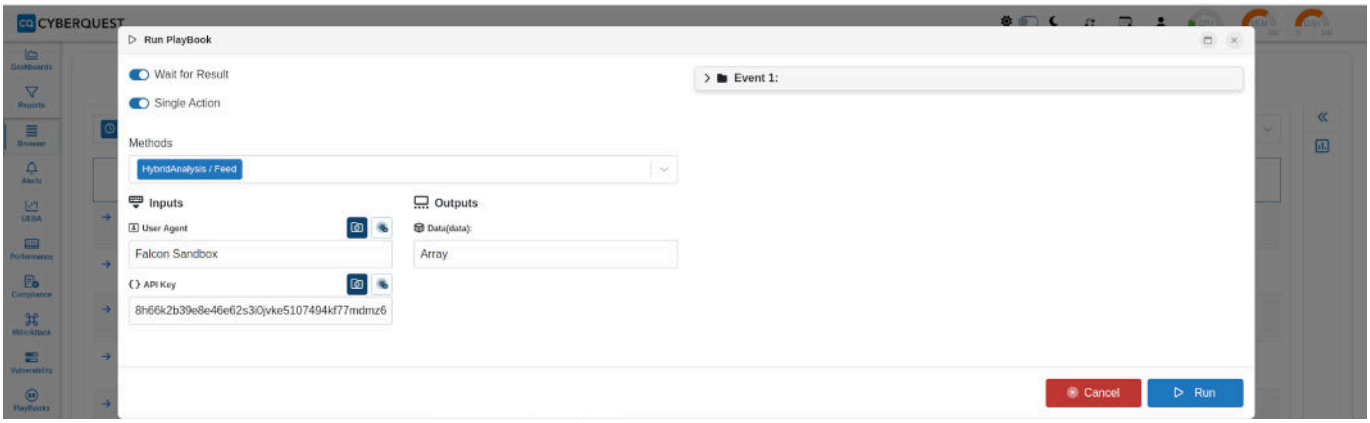


Inputs	Description
User Agent (is required)	Additionally, in order to bypass internal User-Agent blacklist checks, it is recommended to provide a typical User-Agent string or the product name Falcon
API Key (is required)	To use this API you must provide an API Key

Outputs	Description
Detonation(detonation)	Details about usage of API Key
Quick Scan(quick_scan)	DEmails about Quick Scans

HybridAnalysis/Feed method

Access a JSON feed (summary information) of last 250 reports from 24h.

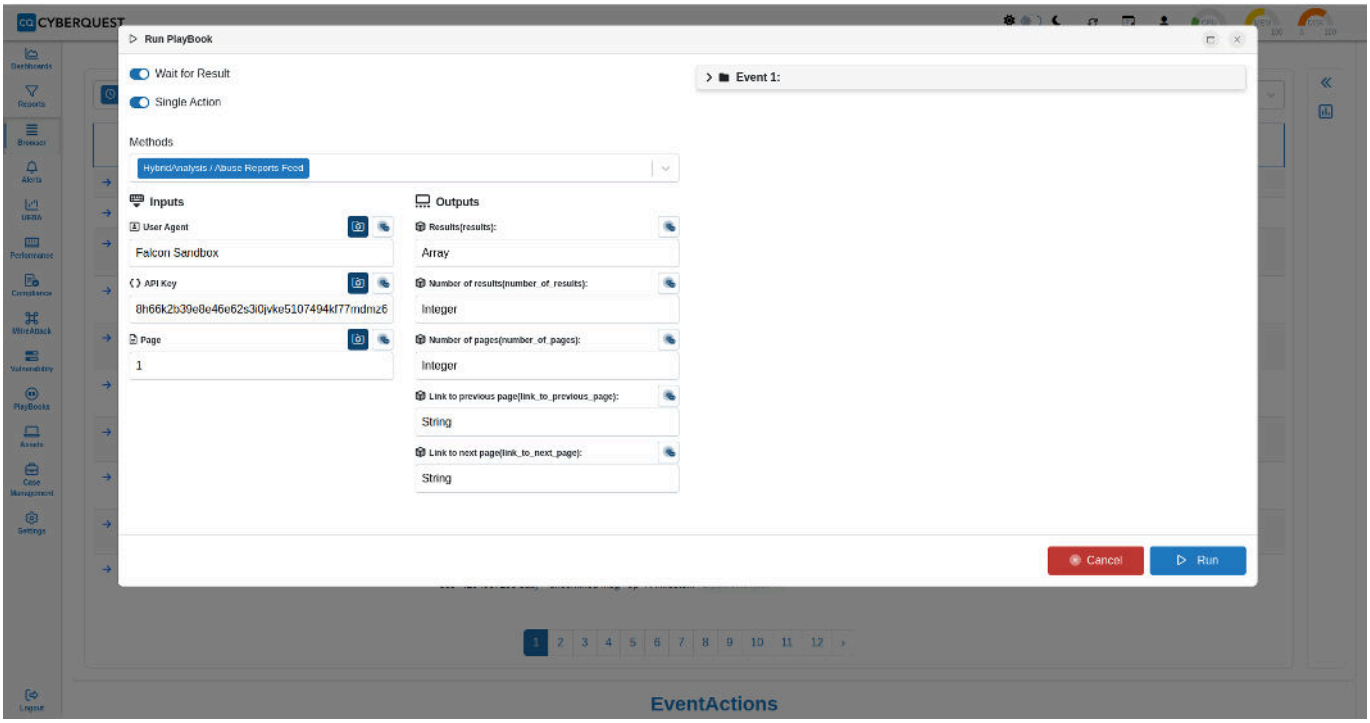


Inputs	Description
User Agent (is required)	Additionally, in order to bypass internal User-Agent blacklist checks, it is recommended to provide a typical User-Agent string or the product name Falcon
API Key (is required)	To use this API you must provide an API Key

Outputs	Description
Data(data)	The results of the aPI call

HybridAnalysis/Abuse Reports Feed method

Returns hashes of samples that were qualified for removal due to abuse or were containing private data and dates when it happened.



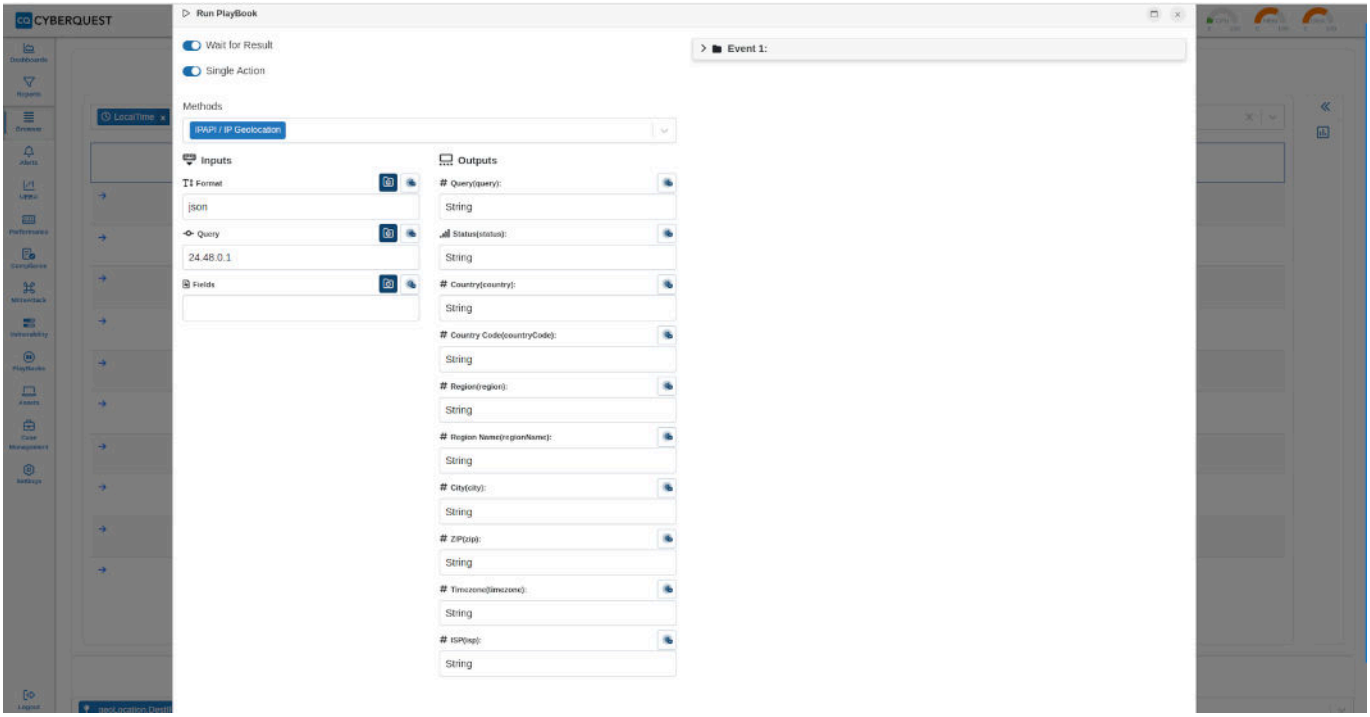
Inputs	Description
User Agent (is required)	Additionally, in order to bypass internal User-Agent blacklist checks, it is recommended to provide a typical User-Agent string or the product name Falcon
API Key (is required)	To use this API you must provide an API Key
Page	Page if there more results than we can display in one request

Outputs	Description
Results(results)	The results of the API call
Number of results(number_of_results)	The total number of results
Number of pages(number_of_pages)	The total number of pages
Link to previous page(link_to_previous_page)	URL to the previous page
Link to next page(link_to_next_page)	URL to the next page

IP-API

IPAPI/IP Geolocation method

Return Geolocation informations.



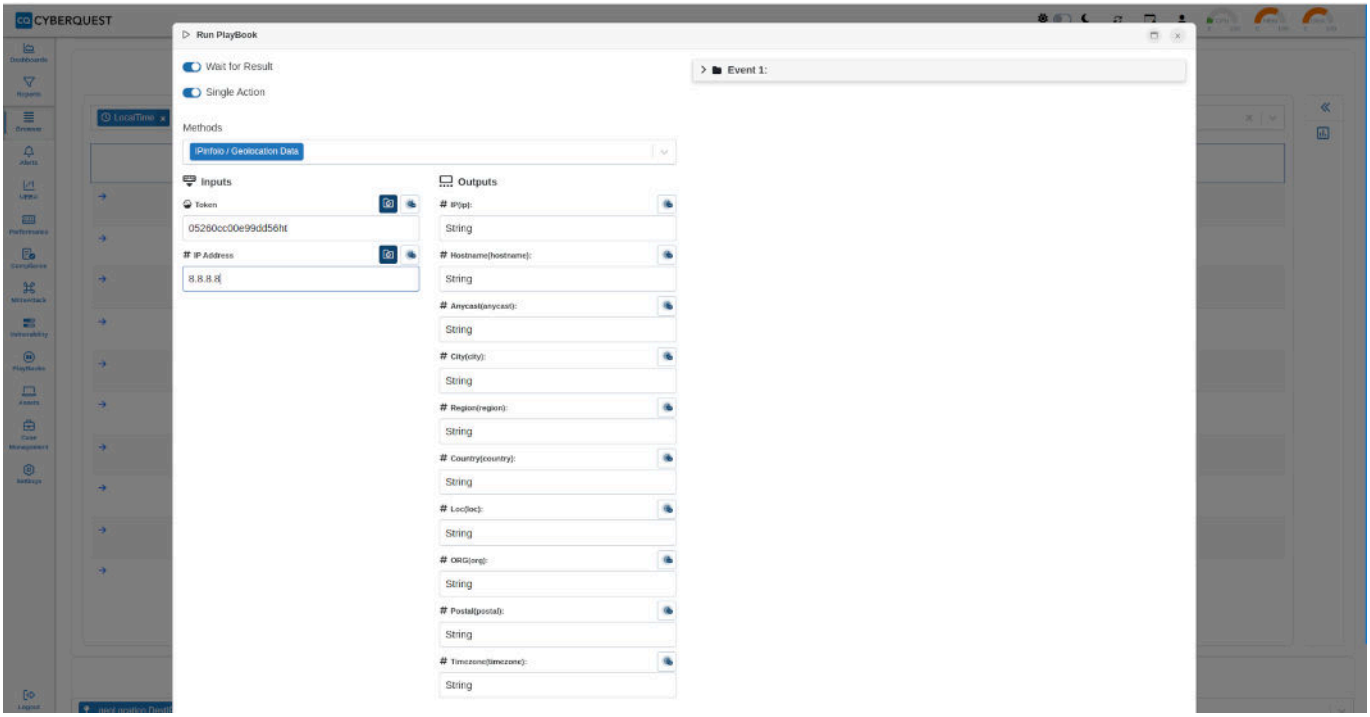
Inputs	Description
Format (is required)	The format in which you want to receive the result
Query	The query can be a single IPv4/IPv6 address or a domain name. If you dont supply a query the current IP address will be used
Fields	If you do not require all the returned fields, use the GET parameter fields to specify which data should be returned

Outputs	Description
Query(query)	The investigated IP
Status(status)	The status of the API call
Country(country)	The country of origin of IP
Country Code(countryCode)	The country code of origin of IP
Region(region)	The region of origin of IP
Region Name(regionName)	The region name of origin of IP
City(city)	The city of origin of IP
ZIP(zip)	The zip of origin of IP
Timezone(timezone)	The timezone of origin of IP
ISP(isp)	The ISP who provided the IP

IPinfo.io

IPinfoio/Geolocation Data method

It includes country, region, city, and postal code of the target IP.



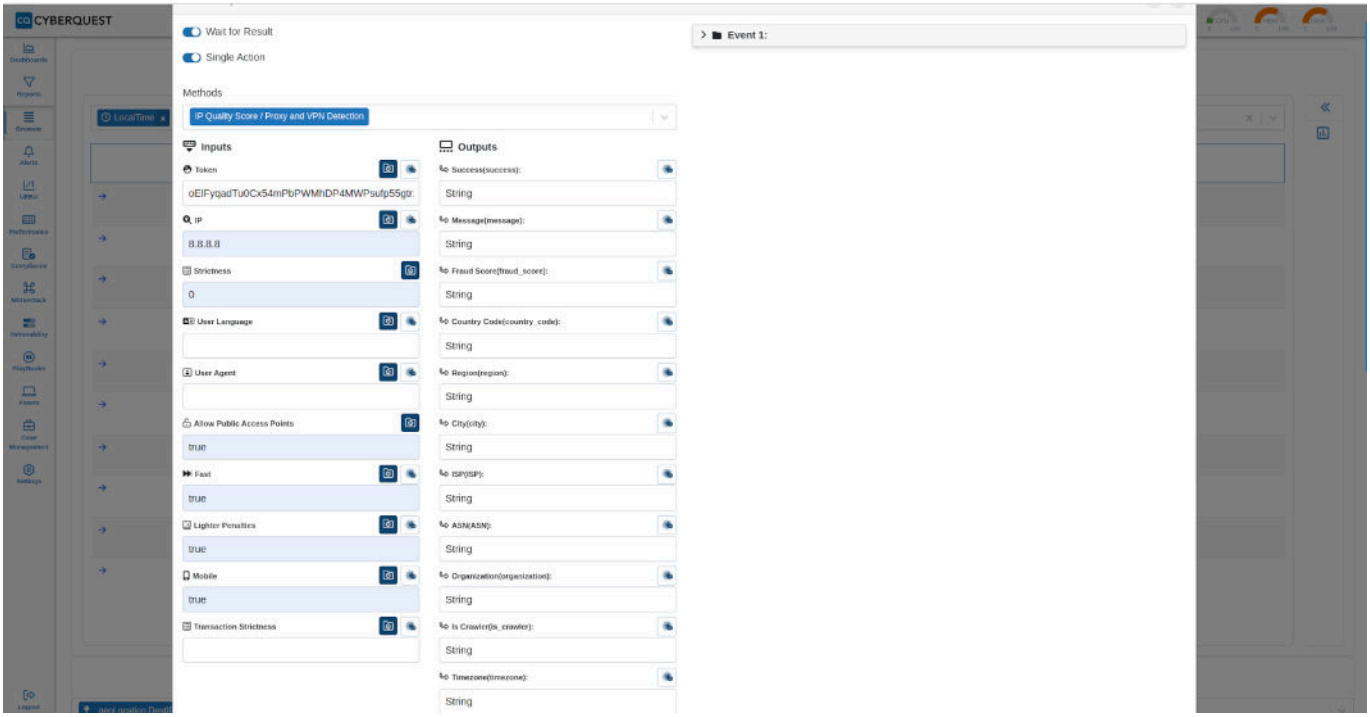
Inputs	Description
Token (is required)	To use the IPinfo.io API, you must have an API key
IP Address (is required)	The IP Address that is being searched

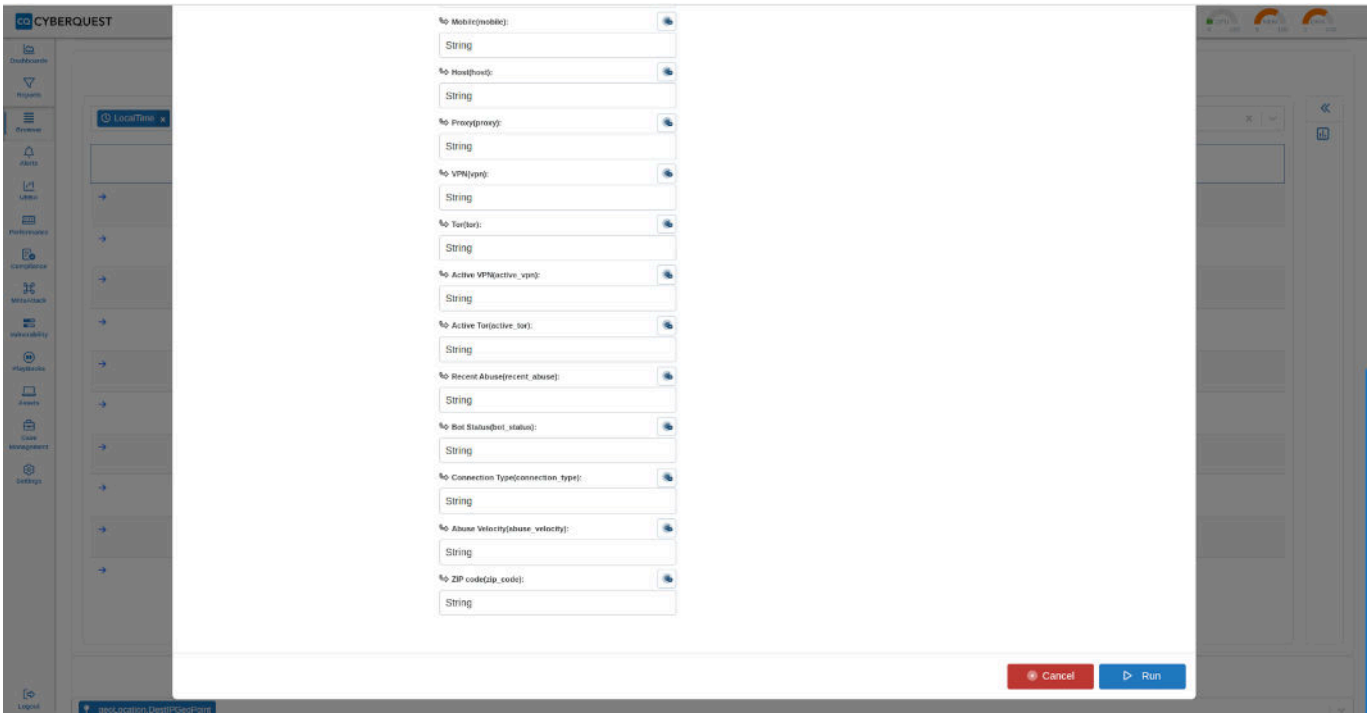
Outputs	Description
IP(ip)	The investigated IP
Hostname(hostname)	Hostname of the investigated IP
Anycast(anycast)	True if the investigated IP is anycast
City(city)	The city of origin of IP
Region(region)	The region of origin of IP
Country(country)	The country of origin of IP
Loc(loc)	The latitude and longitude
ORG(org)	The organisation that issued the IP
Postal(postal)	The postal code of origin of IP
Timezone(timezone)	The timezone of origin of IP

IPQualityScore

IP Quality Score/Proxy and VPN Detection method

List the syslog servers for a network.


CYBERQUEST
Wait for Result
Single Action
Methods
IP Quality Score / Proxy and VPN Detection
Inputs
Outputs
Event 1:
Token
IP
Strictness
User Language
User Agent
Allow Public Access Points
Fast
Lighter Penalties
Mobile
Transaction Strictness
Success(success):
Message(message):
Fraud Score(fraud_score):
Country Code(country_code):
Region(region):
City(city):
ISP(ISP):
ASN(ASN):
Organization(organization):
Is Crawler(is_crawler):
Timezone(timezone):
String
true
8.8.8.8
0

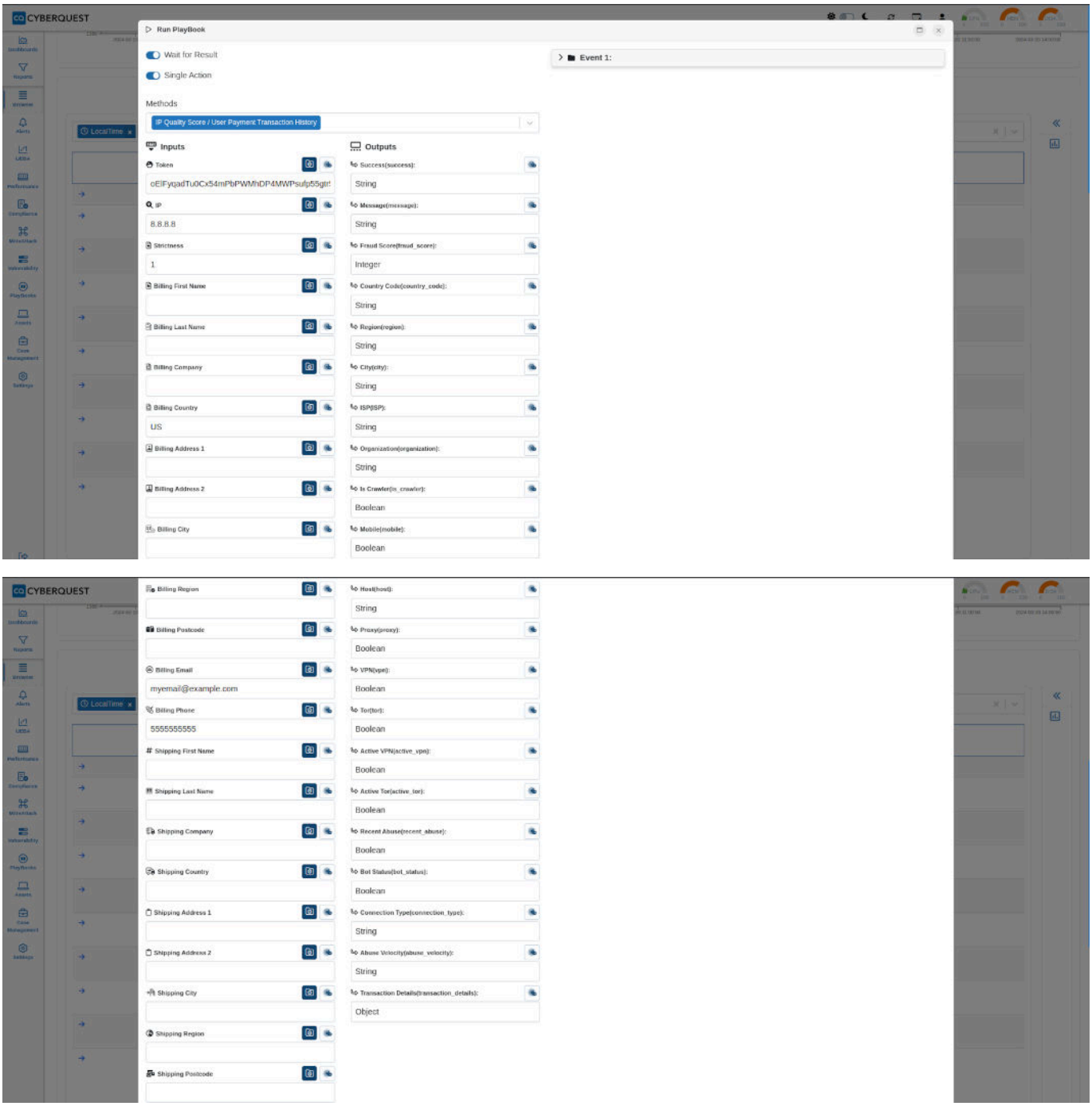

CYBERQUEST
Mobile(mobile):
Host(host):
Proxy(proxy):
VPN(vpn):
Tor(tor):
Active VPN(active_vpn):
Active Tor(active_tor):
Recent Abuse(recent_abuse):
Bot Status(bot_status):
Connection Type(connection_type):
Abuse Velocity(abuse_velocity):
ZIP code(zip_code):
String
Cancel
Run

Inputs	Description
Token (is required)	To use IP Quality Score you need to have an API Key
IP (is required)	The investigated IP
Strictness	
User Language	You can optionally provide us with the users language header. This allows us to evaluate the risk of the user as judged in the fraud_score
User Agent	You can optionally provide us with the user agent string (browser). This allows us to run additional checks to see if the user is a bot or running an invalid browser. This allows us to evaluate the risk of the user as judged in the fraud_score
Allow Public Access Points	
Fast	When this parameter is enabled our API will not perform certain forensic checks that take longer to process. Enabling this feature greatly increases the API speed without much impact on accuracy. This option is intended for services that require decision making in a time sensitive manner and can be used for any strictness level
Lighter Penalties	Is your scoring too strict? Enable this setting to lower detection rates and Fraud Scores for mixed quality IP addresses. If you experience any false-positives with your traffic then enabling this feature will provide better results
Mobile	You can optionally specify that this lookup should be treated as a mobile device. Recommended for mobile lookups that do not have a user agent attached to the request. NOTE: This can cause unexpected and abnormal results if the device is not a mobile device
Transaction Strictness	Adjusts the weights for penalties applied due to irregularities and fraudulent patterns detected on order and transaction details that can be optionally provided on each API request. This feature is only beneficial if you are passing order and transaction details

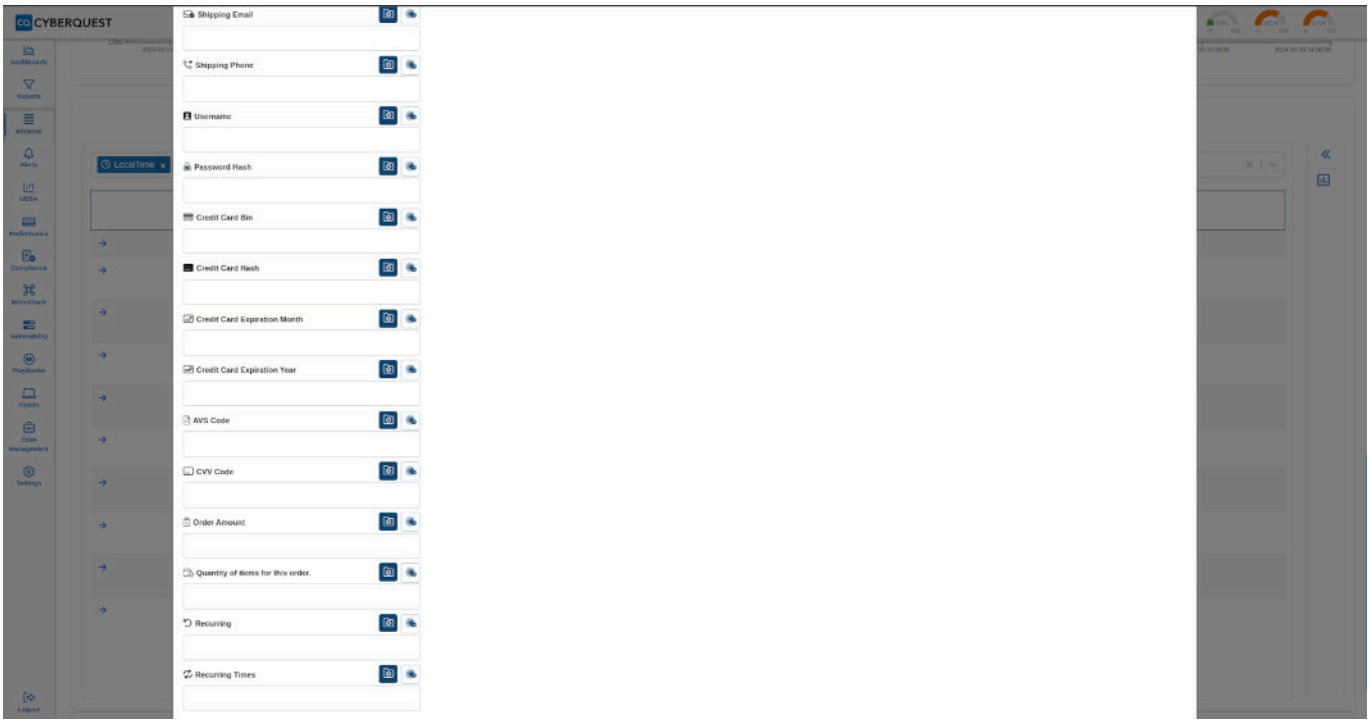
Outputs	Description
Success(success)	Was the request successful?
Message(message)	A generic status message, either success or some form of an error notice
Fraud Score(fraud_score)	The overall fraud score of the user based on the IP, user agent, language, and any other optionally passed variables. Fraud Scores >= 75 are suspicious, but not necessarily fraudulent. We recommend flagging or blocking traffic with Fraud Scores >= 88, but you may find it beneficial to use a higher or lower threshold
Country Code(country_code)	Two character country code of IP address or N/A if unknown
Region(region)	Region (state) of IP address if available or N/A if unknown
City(city)	City of IP address if available or N/Aif unknown
ISP(ISP)	ISP if one is known. Otherwise N/A
ASN(ASN)	Autonomous System Number if one is known. Null if nonexistent
Organization(organization)	Organization if one is known. Can be parent company or sub company of the listed ISP. Otherwise N/A
Is Crawler(is_crawler)	Is this IP associated with being a confirmed crawler from a mainstream search engine such as Googlebot, Bingbot, Yandex, etc. based on hostname or IP address verification
Timezone(timezone)	Timezone of IP address if available or N/A if unknown
Mobile(mobile)	Is this user agent a mobile browser? (will always be false if the user agent is not passed in the API request)
Host(host)	Hostname of the IP address if one is available
Proxy(proxy)	Is this IP address suspected to be a proxy? (SOCKS, Elite, Anonymous, VPN, Tor, etc.)
VPN(vpn)	Is this IP suspected of being a VPN connection? This can include data center ranges which can become active VPNs at any time. The proxy status will always be true when this value is true
Tor(tor)	Is this IP suspected of being a TOR connection? This can include previously active TOR nodes and exits which can become active TOR exits at any time. The proxy status will always be true when this value is true
Active VPN(active_vpn)	Identifies active VPN connections used by popular VPN services and private VPN servers
Active Tor(active_tor)	Identifies active TOR exits on the TOR network
Recent Abuse(recent_abuse)	This value will indicate if there has been any recently verified abuse across our network for this IP address. Abuse could be a confirmed chargeback, compromised device, fake app install, or similar malicious behavior within the past few days
Bot Status(bot_status)	Indicates if bots or non-human traffic has recently used this IP address to engage in automated fraudulent behavior. Provides stronger confidence that the IP address is suspicious
Connection Type(connection_type)	Classification of the IP address connection type as Residential, Corporate, Education, Mobile, or Data Center
Abuse Velocity(abuse_velocity)	How frequently the IP address is engaging in abuse across the IPQS threat network. Values can be high, medium, low, or none. Can be used in combination with the Fraud Score to identify bad behavior
ZIP code(zip_code)	Postal code of IP address if available or N/A if unknown. IP addresses can relate to multiple postal codes in a city, so we recommend performing analysis of similar postal codes nearby

IP Quality Score/User Payment Transaction History method

User Payment Transaction History.


CYBERQUEST
Run PlayBook
Wait for Result
Single Action
Event 1:
Methods
IP Quality Score / User Payment Transaction History
Inputs
Outputs
Token
oElFyqadTu0Cx54mPbPWMhDP4MWPsufp55gtr
IP
8.8.8.8
Strictness
1
Billing First Name
Billing Last Name
Billing Company
Billing Country
US
Billing Address 1
Billing Address 2
Billing City
Success(success):
String
Message(message):
String
Fraud Score(fraud_score):
Integer
Country Code(country_code):
String
Region(region):
String
City(city):
String
ISP(ISP):
String
Organization(organization):
String
Is Crawler(is_crawler):
Boolean
Mobile(mobile):
Boolean

CYBERQUEST
Billing Region
Billing Postcode
Billing Email
myemail@example.com
Billing Phone
5555555555
Shipping First Name
Shipping Last Name
Shipping Company
Shipping Country
Shipping Address 1
Shipping Address 2
Shipping City
Shipping Region
Shipping Postcode
Host(host):
String
Proxy(proxy):
Boolean
VPN(vpn):
Boolean
Tor(tor):
Boolean
Active VPN(active_vpn):
Boolean
Active Tor(active_tor):
Boolean
Recent Abuse(recent_abuse):
Boolean
Bot Status(bot_status):
Boolean
Connection Type(connection_type):
String
Abuse Velocity(abuse_velocity):
String
Transaction Details(transaction_details):
Object


CYBERQUEST
Shipping Email
Shipping Phone
Username
Password Hash
Credit Card Bin
Credit Card Hash
Credit Card Expiration Month
Credit Card Expiration Year
AVS Code
CVV Code
Order Amount
Quantity of items for this order.
Recurring
Recurring Times

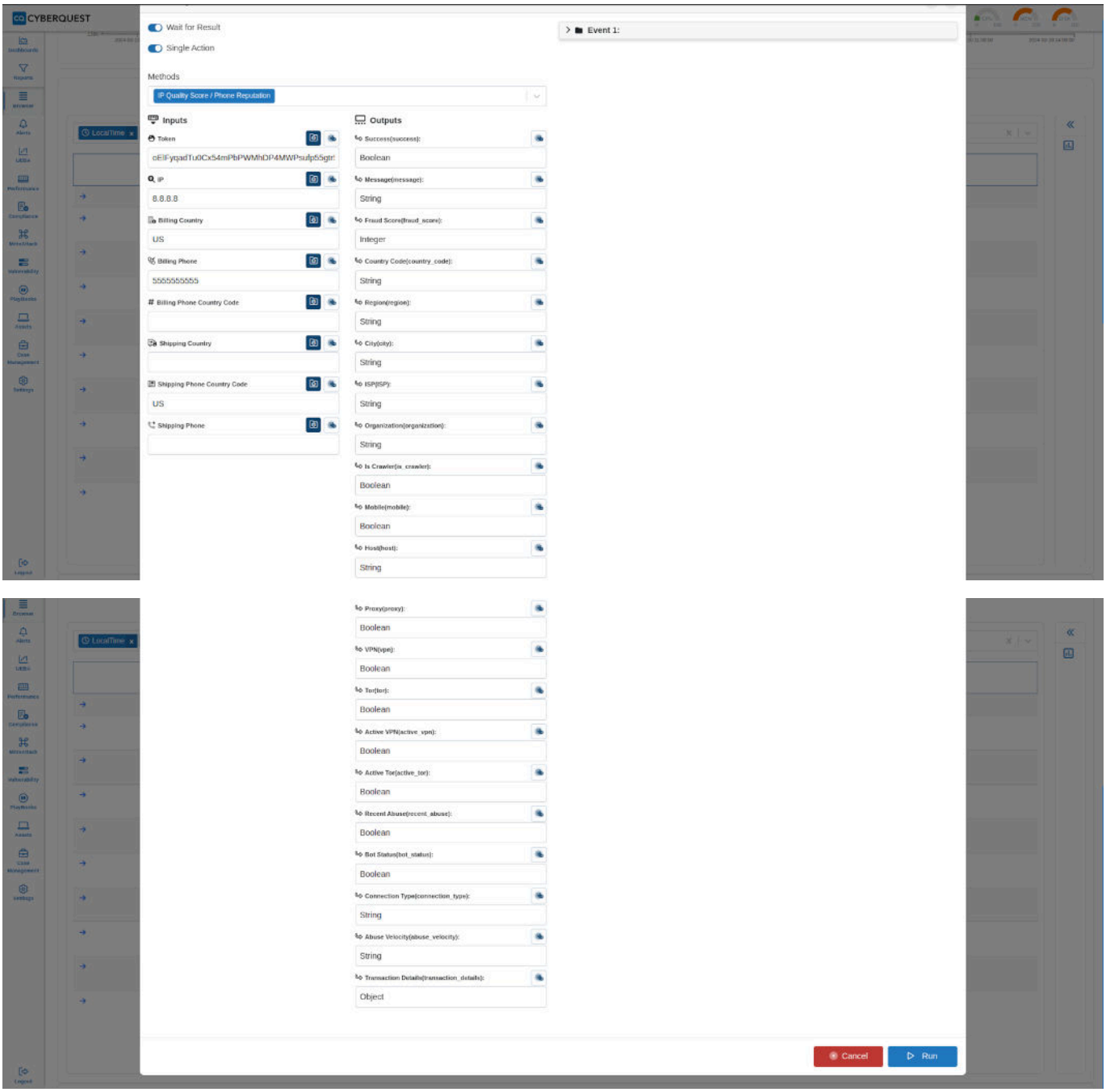
Inputs	Description
Token (is required)	To use IP Quality Score you need to have an API Key
IP (is required)	The investigated IP
Strictness	Uses the lowest strictness (0-3) for Fraud Scoring. Increasing this value will expand the tests we perform. Levels 2+ have a higher risk of false-positives. We recommend using level 0 or 1 for the best results
Billing First Name	The customers billing first name
Billing Last Name	The customers billing last name
Billing Company	The customers billing company
Billing Country	The customers billing country name or billing country ISO-Alpha2. (EG: United States or US)
Billing Address 1	The customers billing street address part 1
Billing Address 2	The customers billing street address part 2
Billing City	The customers billing city
Billing Region	The customers billing region or state
Billing Postcode	The customers billing postcode or zipcode
Billing Email	The customers billing email address
Billing Phone	The customers billing 11 to 14 digit phone number. (If less than 10 digits provided, the country code will be guessed by IP Quality Score AI.)
Shipping First Name	The customers shipping first name
Shipping Last Name	The customers shipping last name
Shipping Company	The customers shipping company
Shipping Country	The customers shipping country name or shipping country ISO-Alpha2. (EG: United States or US)
Shipping Address 1	The customers shipping street address part 1
Shipping Address 2	The customers shipping street address part 2
Shipping City	The customers shipping city
Shipping Region	The customers shipping region or state
Shipping Postcode	The customers shipping postcode or zipcode
Shipping Email	The customers shipping email address
Shipping Phone	The customers shipping phone number
Username	The customers username
Password Hash	For security reasons and following industry best practices, a SHA256 hash of the users password for better user analysis
Credit Card Bin	First six digits of the credit or debit card, referred to ask the Bank Identification Number
Credit Card Hash	For security reasons and following industry best practices, a SHA256 hash of the credit card number is accepted to check against blacklisted cards
Credit Card Expiration Month	Two letter format of the credit cards expiration month. For example, May would be 05
Credit Card Expiration Year	Two letter format of the credit cards expiration year. For example, 2023 would be 23

Inputs	Description
AVS Code	One letter Address Verification Service (AVS) response code provided by the credit card processor or bank
CVV Code	One letter Card Verification Value (CVV2) response code provided by the credit card processor or bank
Order Amount	Total balance of the entire order without currency symbols
Quantity of items for this order	Quantity of items for this order
Recurring	Is this a recurring order that automatically rebills?
Recurring Times	If this is a recurring order, then how many times has this recurring order rebilled? For example, if this is the third time the user is being billed, please enter this value as 3. If this is the initial recurring order, please leave the value as blank or enter 1

Outputs	Description
Success(success)	Was the request successful?
Message(message)	A generic status message, either success or some form of an error notice
Fraud Score(fraud_score)	The overall fraud score of the user based on the IP, user agent, language, and any other optionally passed variables. Fraud Scores >= 75 are suspicious, but not necessarily fraudulent. We recommend flagging or blocking traffic with Fraud Scores >= 88, but you may find it beneficial to use a higher or lower threshold
Country Code(country_code)	Two character country code of IP address or N/A if unknown
Region(region)	Region (state) of IP address if available or N/A if unknown
City(city)	City of IP address if available or N/A if unknown
ISP(ISP)	ISP if one is known. Otherwise N/A
Organization(organization)	Organization if one is known. Can be parent company or sub company of the listed ISP. Otherwise N/A
Is Crawler(is_crawler)	Is this IP associated with being a confirmed crawler from a mainstream search engine such as Googlebot, Bingbot, Yandex, etc. based on hostname or IP address verification.
Mobile(mobile)	Is this user agent a mobile browser? (will always be false if the user agent is not passed in the API request)
Host(host)	Hostname of the IP address if one is available
Proxy(proxy)	Is this IP address suspected to be a proxy? (SOCKS, Elite, Anonymous, VPN, Tor, etc.)
VPN(vpn)	Is this IP suspected of being a VPN connection? This can include data center ranges which can become active VPNs at any time. The proxy status will always be true when this value is true
Tor(tor)	Is this IP suspected of being a TOR connection? This can include previously active TOR nodes and exits which can become active TOR exits at any time. The proxy status will always be true when this value is true
Active VPN(active_vpn)	Identifies active VPN connections used by popular VPN services and private VPN servers
Active Tor(active_tor)	Identifies active TOR exits on the TOR network
Recent Abuse(recent_abuse)	This value will indicate if there has been any recently verified abuse across our network for this IP address. Abuse could be a confirmed chargeback, compromised device, fake app install, or similar malicious behavior within the past few days
Bot Status(bot_status)	Indicates if bots or non-human traffic has recently used this IP address to engage in automated fraudulent behavior. Provides stronger confidence that the IP address is suspicious
Connection Type(connection_type)	Classification of the IP address connection type as Residential, Corporate, Education, Mobile, or Data Center
Abuse Velocity(abuse_velocity)	How frequently the IP address is engaging in abuse across the IPQS threat network. Values can be high, medium, low, or none. Can be used in combination with the Fraud Score to identify bad behavior
Transaction Details(transaction_details)	Physical address validation and reputation analysis

IP Quality Score/Phone Reputation method

Generate a phone number reputation score to verify users, payments, & sign ups to prevent fraudulent behavior.

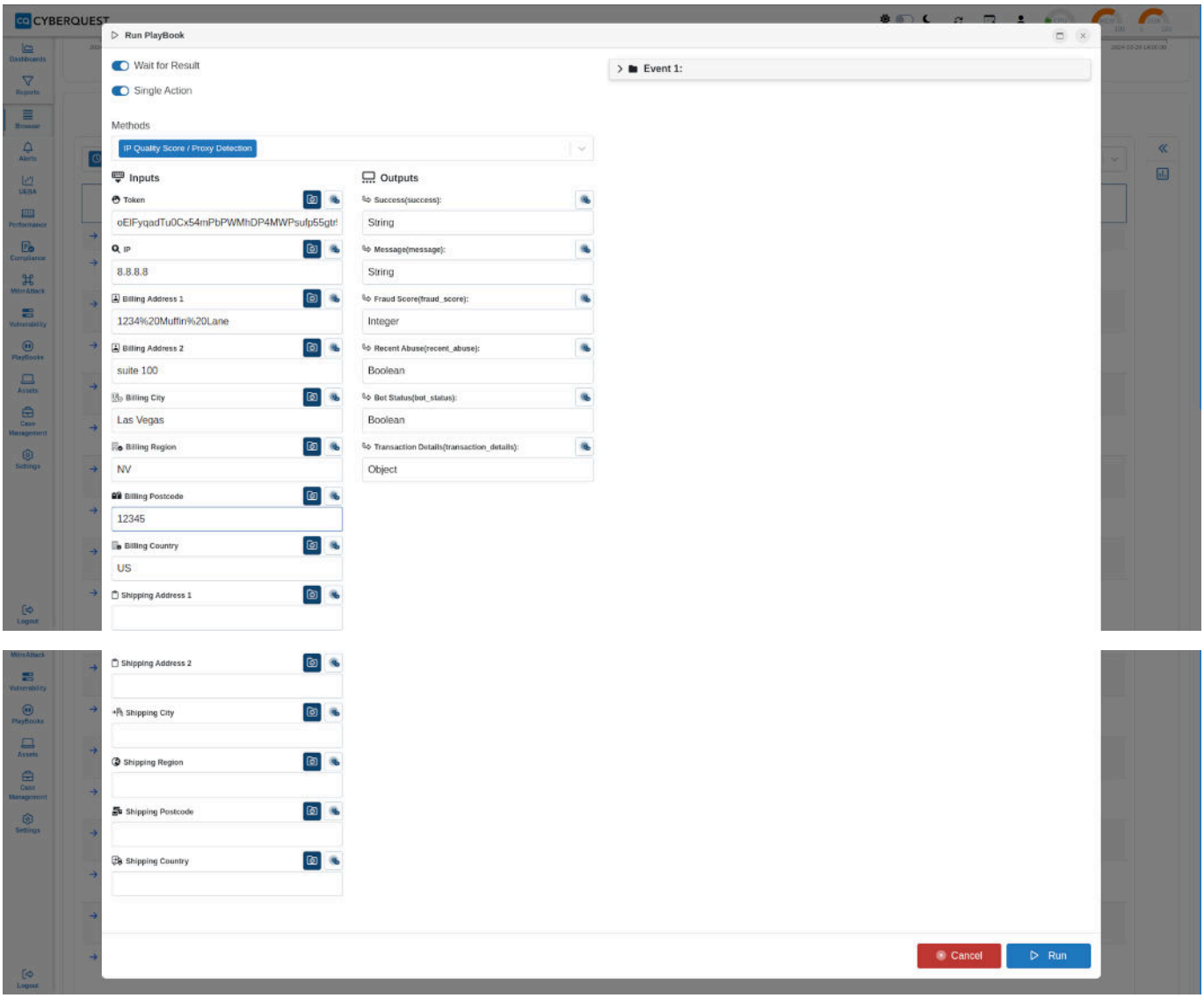


Inputs	Description
Token (is required)	To use IP Quality Score you need to have an API Key
IP (is required)	The investigated IP
Billing Country	The customers billing country name or billing country ISO-Alpha2. (EG: United States or US)
Billing Phone	The customers billing 11 to 14 digit phone number. (If less than 10 digits provided, the country code will be guessed by IP Quality Score AI.)
Billing Phone Country Code	Country dialing code associated with the billing phone. Typically 1-3 digits
Shipping Country	The customers shipping country name or shipping country ISO-Alpha2. (EG: United States or US)
Shipping Phone Country Code	Country dialing code associated with the shipping phone. Typically 1-3 digits
Shipping Phone	The customers shipping phone number

Outputs	Description
Success(success)	Was the request successful?
Message(message)	A generic status message, either success or some form of an error notice
Fraud Score(fraud_score)	The overall fraud score of the user based on the IP, user agent, language, and any other optionally passed variables. Fraud Scores >= 75 are suspicious, but not necessarily fraudulent. We recommend flagging or blocking traffic with Fraud Scores >= 88, but you may find it beneficial to use a higher or lower threshold
Country Code(country_code)	Two character country code of IP address or N/A if unknown
Region(region)	Region (state) of IP address if available or N/A if unknown
City(city)	City of IP address if available or N/A if unknown
ISP(ISP)	ISP if one is known. Otherwise N/A
Organization(organization)	Organization if one is known. Can be parent company or sub company of the listed ISP. Otherwise N/A
Is Crawler(is_crawler)	Is this IP associated with being a confirmed crawler from a mainstream search engine such as Googlebot, Bingbot, Yandex, etc. based on hostname or IP address verification
Mobile(mobile)	Is this user agent a mobile browser? (will always be false if the user agent is not passed in the API request)
Host(host)	Hostname of the IP address if one is available
Proxy(proxy)	Is this IP address suspected to be a proxy? (SOCKS, Elite, Anonymous, VPN, Tor, etc.)
VPN(vpn)	Is this IP suspected of being a VPN connection? This can include data center ranges which can become active VPNs at any time. The proxy status will always be true when this value is true
Tor(tor)	Is this IP suspected of being a TOR connection? This can include previously active TOR nodes and exits which can become active TOR exits at any time. The proxy status will always be true when this value is true
Active VPN(active_vpn)	Identifies active VPN connections used by popular VPN services and private VPN servers
Active Tor(active_tor)	Identifies active TOR exits on the TOR network
Recent Abuse(recent_abuse)	This value will indicate if there has been any recently verified abuse across our network for this IP address. Abuse could be a confirmed chargeback, compromised device, fake app install, or similar malicious behavior within the past few days
Bot Status(bot_status)	Indicates if bots or non-human traffic has recently used this IP address to engage in automated fraudulent behavior. Provides stronger confidence that the IP address is suspicious
Connection Type(connection_type)	Classification of the IP address connection type as Residential, Corporate, Education, Mobile, or Data Center
Abuse Velocity(abuse_velocity)	How frequently the IP address is engaging in abuse across the IPQS threat network. Values can be high, medium, low, or none. Can be used in combination with the Fraud Score to identify bad behavior
Transaction Details(transaction_details)	A generic status message, either success or some form of an error notice

IP Quality Score /Proxy Detection method

Instantly detect invalid addresses, misformatted user data and typos, and physical addresses that have recently been reported for fraudulent behavior.

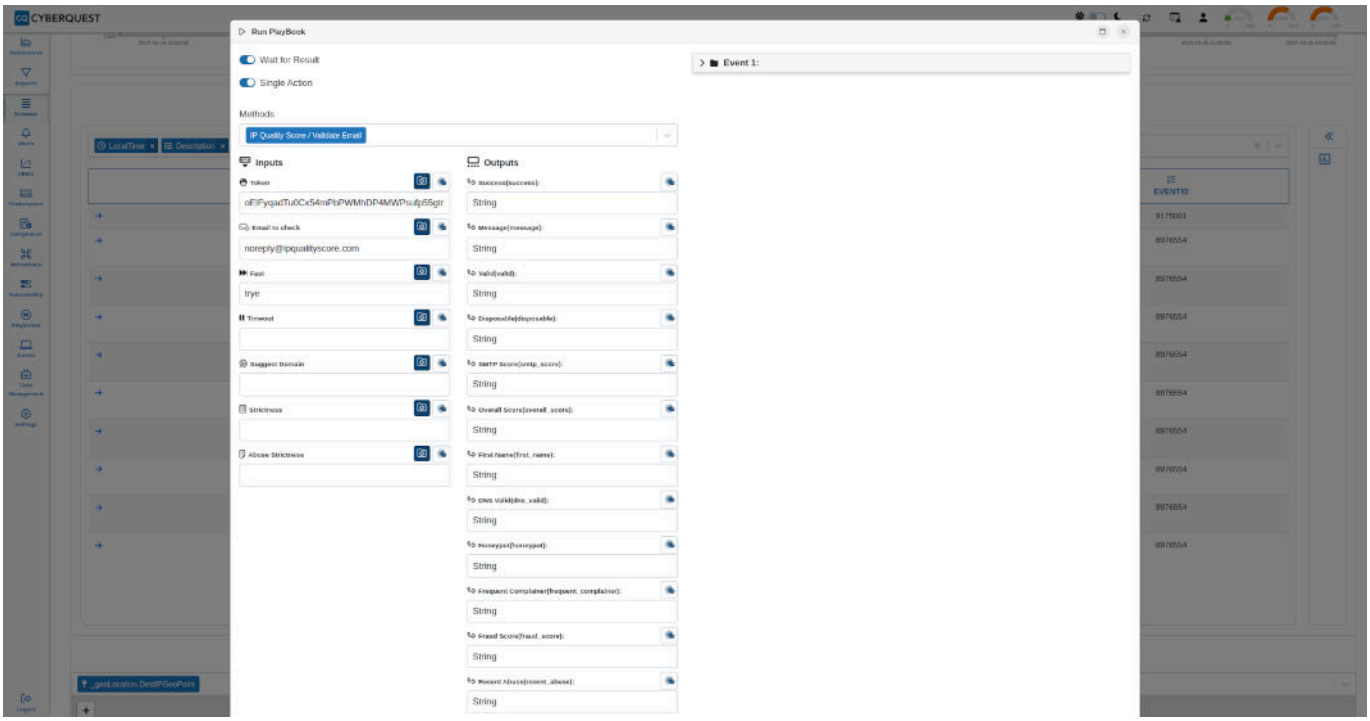


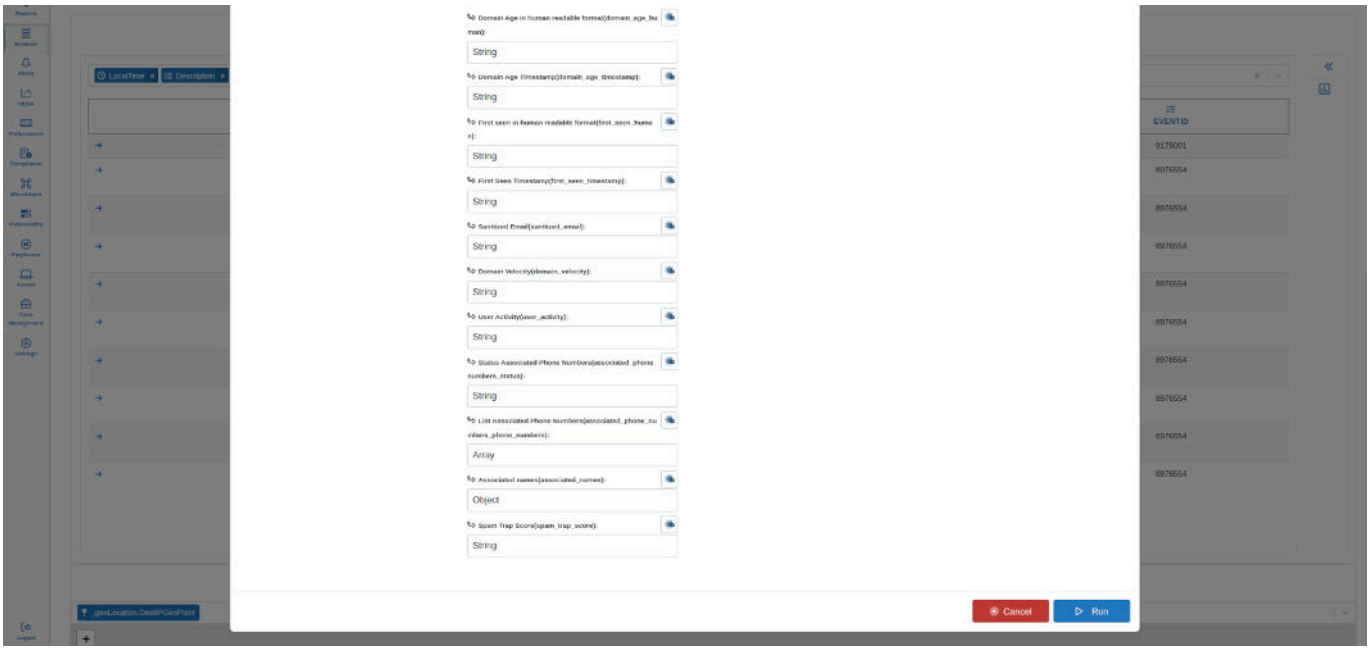
Inputs	Description
Token (is required)	To use IP Quality Score you need to have an API Key
IP (is required)	The investigated IP
Billing Address 1	Users billing or primary street address part 1.
Billing Address 2	Users billing or primary street address part 2.
Billing City	Users billing or primary city.
Billing Region	Users billing or primary region or state.
Billing Postcode	Users billing or primary postcode or zipcode.
Billing Country	Users billing or primary country name or billing country ISO-Alpha2. (EG: United States or US)
Shipping Address 1	Users billing or primary street address part 1.
Shipping Address 2	Users billing or primary street address part 2.
Shipping City	Users billing or primary city.
Shipping Region	Users billing or primary region or state.
Shipping Postcode	Users billing or primary postcode or zipcode.
Shipping Country	Users billing or primary country name or shipping country ISO-Alpha2. (EG: United States or US)

Outputs	Description
Success (success)	Was the request successful?
Message (message)	A generic status message, either success or some form of an error notice.
Fraud Score (fraud_score)	The overall fraud score of the user based on the IP, user agent, language, and any other optionally passed variables. Fraud Scores >= 75 are suspicious, but not necessarily fraudulent. We recommend flagging or blocking traffic with Fraud Scores >= 88, but you may find it beneficial to use a higher or lower threshold.
Recent Abuse (recent_abuse)	This value will indicate if there has been any recently verified abuse across our network for this IP address. Abuse could be a confirmed chargeback, compromised device, fake app install, or similar malicious behavior within the past few days.
Bot Status (bot_status)	Indicates if bots or non-human traffic has recently used this IP address to engage in automated fraudulent behavior. Provides stronger confidence that the IP address is suspicious.
Transaction Details (transaction_details)	Physical address validation and reputation analysis.

IP Quality Score /Validate Email method

IPQualityScores Email Validation API boosts deliverability by detecting invalid, fraudulent emails, spam traps, and more. It offers real-time verification to prevent fake accounts, errors, and misuse on your platform.





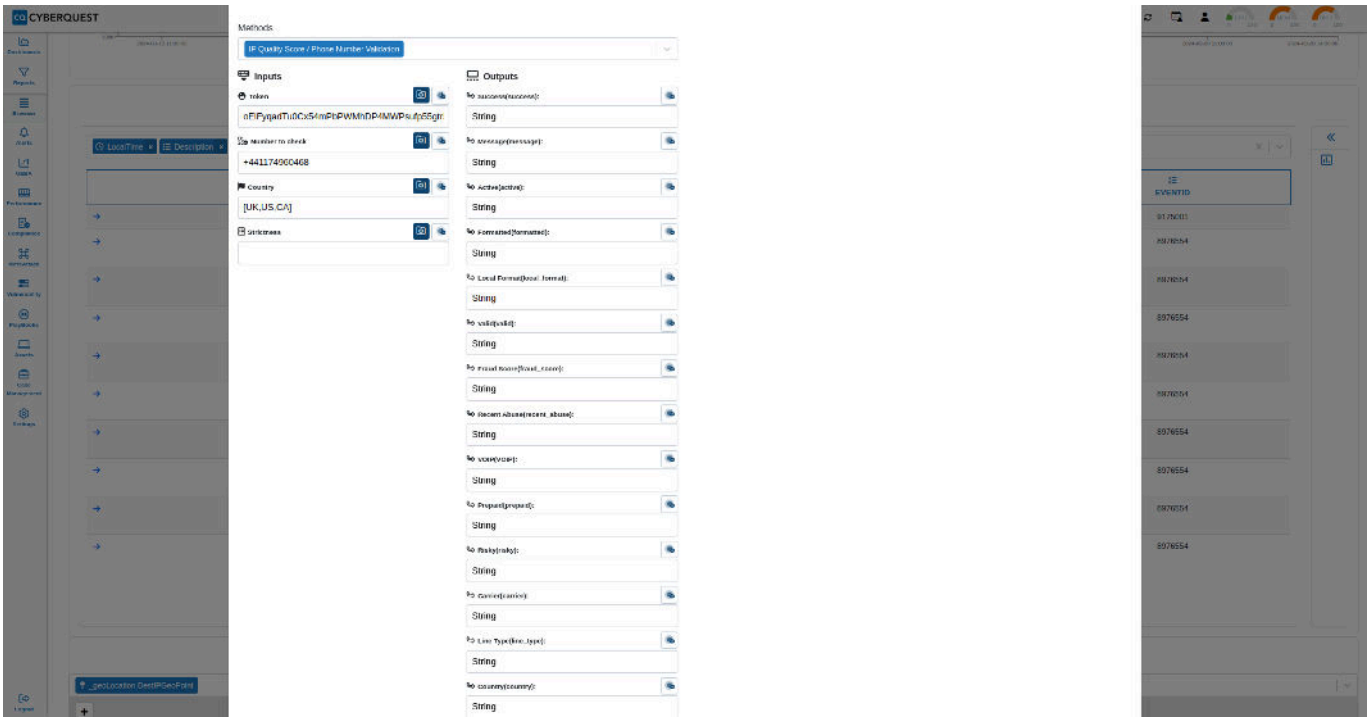
Inputs	Description
Token (is required)	To use IP Quality Score you need to have an API Key
Email to check (is required)	The email which is verified
Fast	When this parameter is enabled our API will not perform an SMTP check with the mail service provider, which greatly increases the API speed. Syntax and DNS checks are still performed on the email address as well as our disposable email detection service. This option is intended for services that require decision making in a time sensitive manner.
Timeout	Maximum number of seconds to wait for a reply from a mail service provider. If your implementation requirements do not need an immediate response, we recommend bumping this value to 20. Any results which experience a connection timeout will return the timed_out variable as true. Default value is 7 seconds.
Suggest Domain	Force analyze if the email addresss domain has a typo and should be corrected to a popular mail service. By default, this test is currently only performed when the email is invalid or if the recent abuse status is true.
Strictness	Sets how strictly spam traps and honeypots are detected by our system, depending on how comfortable you are with identifying emails suspected of being a spam trap. 0 is the lowest level which will only return spam traps with high confidence. Strictness levels above 0 will return increasingly more strict results, with level 2 providing the greatest detection rates.
Abuse Strictness	Set the strictness level for machine learning pattern recognition of abusive email addresses with the recent_abuse data point. Default level of 0 provides good coverage, however if you are filtering account applications and facing advanced fraudsters then we recommend increasing this value to level 1 or 2.

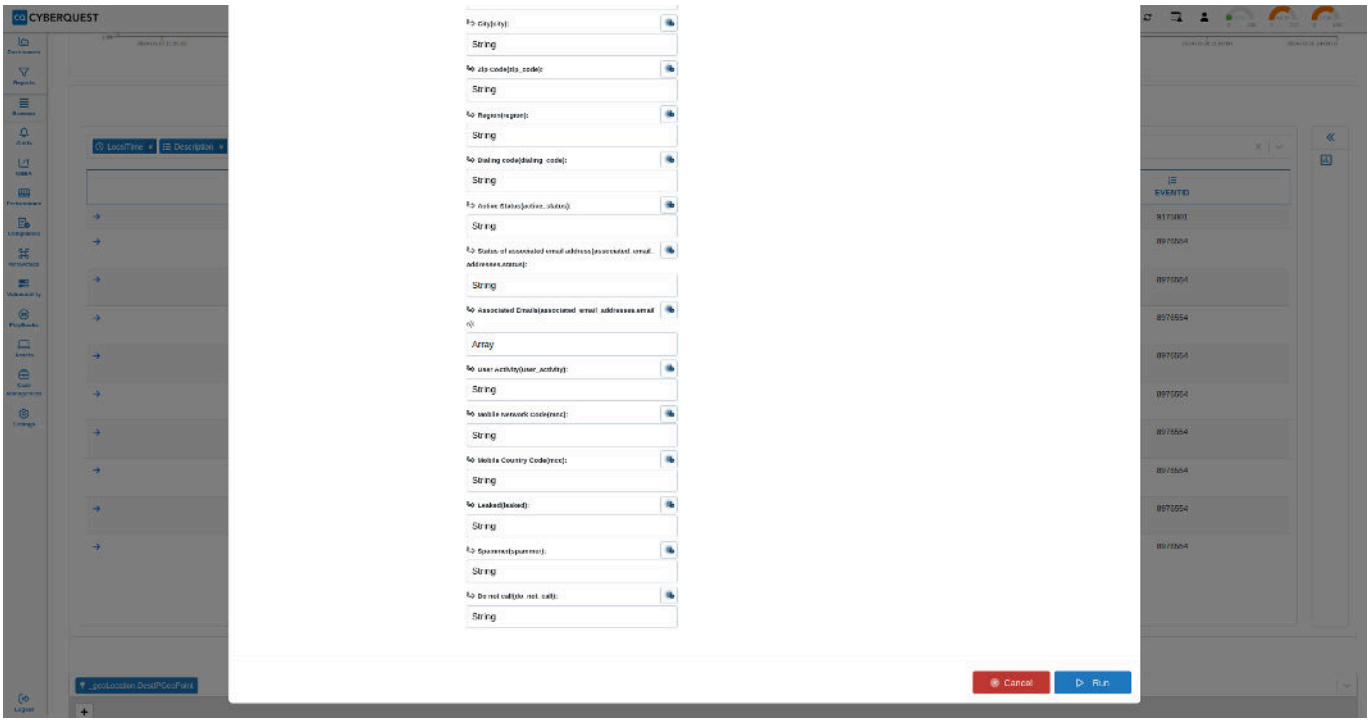
Outputs	Description
Success (success)	Was the request successful?
Message (message)	A generic status message, either success or some form of an error notice.
Valid (valid)	Does this email address appear valid?
Disposable (disposable)	Is this email suspected of belonging to a temporary or disposable mail service? Usually associated with fraudsters and scammers.
SMTP Score (smtp_score)	Validity score of email servers SMTP setup. Range: -1 - 3. Scores above -1 can be associated with a valid email.-1 = invalid email address0 = mail server exists, but is rejecting all mail1 = mail server exists, but is showing a temporary error2 = mail server exists, but accepts all email3 = mail server exists and has verified the email address
Overall Score (overall_score)	Overall email validity score. Range: 0 - 4. Scores above 1 can be associated with a valid email.0 = invalid email address1 = dns valid, unreachable mail server2 = dns valid, temporary mail rejection error3 = dns valid, accepts all mail4 = dns valid, verified email exists
First Name (first_name)	Suspected first name based on email. Returns CORPORATE if the email is suspected of being a generic company email. Returns UNKNOWN if the first name was not determinable.
DNS Valid (dns_valid)	Does the emails hostname have valid DNS entries? Partial indication of a valid email.
Honeypot (honeypot)	Is this email believed to be a honeypot or SPAM trap? Bulk mail sent to these emails increases your risk of being blacklisted by large ISPs & ending up in the spam folder.
Frequent Complainer (frequent_complainer)	Indicates if this email frequently unsubscribes from marketing lists or reports email as SPAM.
Fraud Score (fraud_score)	The overall Fraud Score of the user based on the emails reputation and recent behavior across the IPQS threat network. Fraud Scores >= 75 are suspicious, but not necessarily fraudulent.
Recent Abuse (recent_abuse)	This value will indicate if there has been any recently verified abuse across our network for this email address. Abuse could be a confirmed chargeback, fake signup, compromised device, fake app install, or similar malicious behavior within the past few days.
Domain Age in human readable format (domain_age_human)	A human description of when this domain was registered. (Ex: 3 months ago)
Domain Age Timestamp (domain_age_timestamp)	The unix time since epoch when this domain was first registered. (Ex: 1568061634)
First seen in human readable format (first_seen_human)	A human description of the email address age, using an estimation of the email creation date when IPQS first discovered this email address. (Ex: 3 months ago)
First Seen Timestamp (first_seen_timestamp)	The unix time since epoch when this email was first analyzed by IPQS. (Ex: 1568061634)
Sanitized Email (sanitized_email)	Sanitized email address with all aliases and masking removed, such as multiple periods for Gmail.com.
Domain Velocity (domain_velocity)	Indicates the level of legitimate users interacting with the email address domain. Values can be high, medium, low, or none. Domains like IBM.com, Microsoft.com, Gmail.com, etc. will have high scores as this value represents popular domains. New domains or domains that are not frequently visited by legitimate users will have a value as none.
User Activity (user_activity)	Frequency at which this email address makes legitimate purchases, account registrations, and engages in legitimate user behavior online. Values can be high, medium, low, or none. Values of high or medium are

Outputs	Description
	strong signals of healthy usage. New email addresses without a history of legitimate behavior will have a value as none. This field is restricted to higher plan tiers.
Status Associated Phone Numbers (associated_phone_numbers_status)	Status of phone numbers associated with investigated email address
List Associated Phone Numbers (associated_phone_numbers_phone_numbers)	A list with associated phone numbers with investigated email address
Associated names (associated_names)	Displays first and last names linked to the email address, if available in our data sources. Match rates vary by country. This field is restricted to upgraded plans. Object value contains, status, and names as an array.
Spam Trap Score (spam_trap_score)	Intelligent confidence level of the email address being an active SPAM trap. Values can be high, medium, low, or none. We recommend scrubbing emails with a high status, typically for any promotional mailings. This data is meant to provide a more accurate result for the frequent_complainer and honeypot data points, which collect data from spam complaints, spam traps, and similar techniques.

IP Quality Score /Phone Number Validation

Perform carrier lookups by API in any region to detect disconnected phone numbers and retrieve important carrier info including line types to determine if a number is a VOIP, landline, mobile.





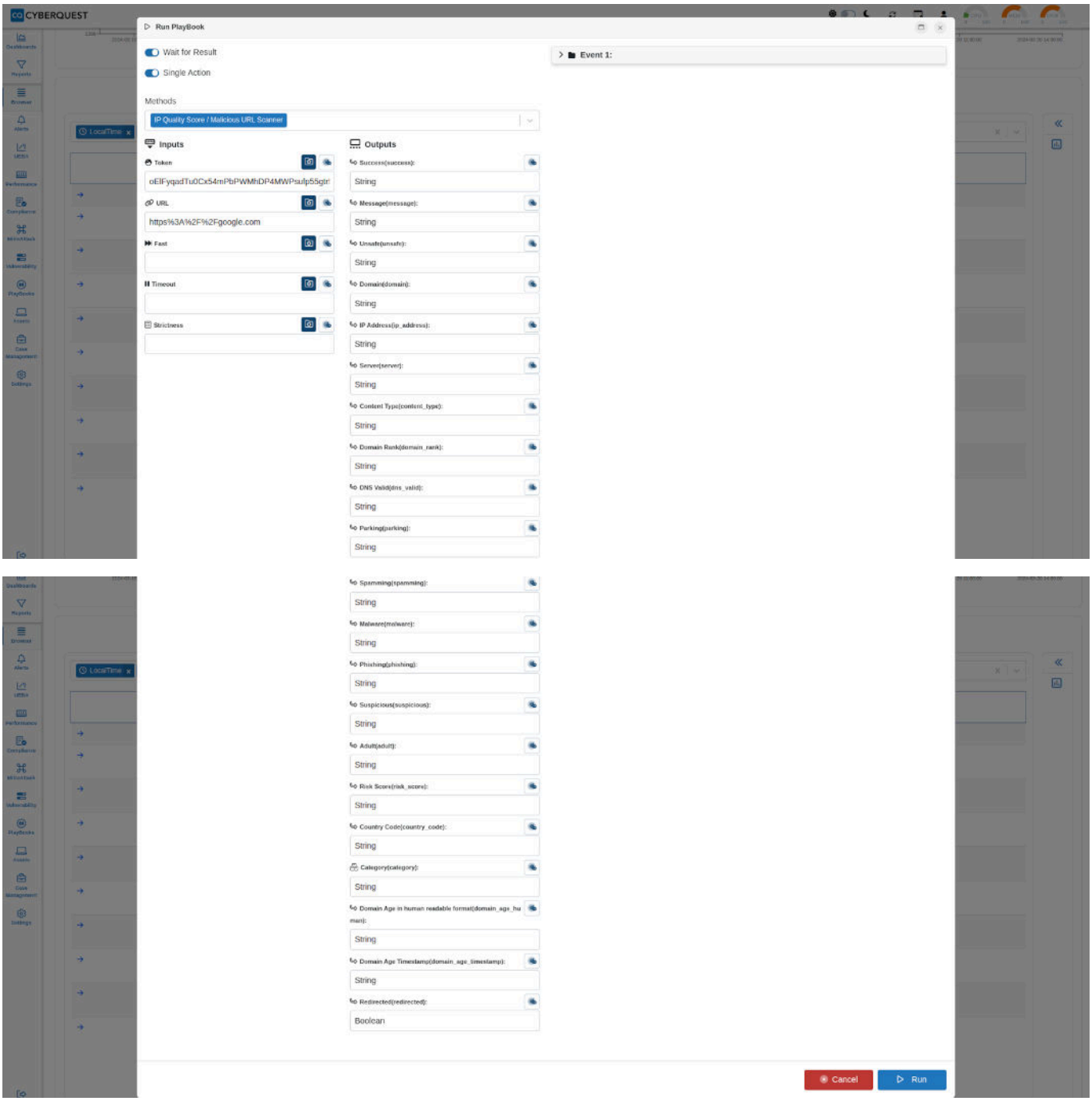
Inputs	Description
Token (is required)	To use IP Quality Score you need to have an API Key
Number to check (is required)	To use IP Quality Score you need to have an API Key
Country	You can optionally provide us with the default country or countries this phone number is suspected to be associated with. Our system will prefer to use a country on this list for verification or will require a country to be specified in the event the phone number is less than 10 digits.
Strictness	How in depth (strict) do you want this reputation check to be? Stricter checks may provide a higher false-positive rate. We recommend starting at 0, the lowest strictness setting, and increasing to 1 or 2 depending on your levels of fraud.

Outputs	Description
Success (success)	Was the request successful?
Message (message)	A generic status message, either success or some form of an error notice.
Active (active)	Is this phone number a live usable phone number that is currently active?
Formatted (formatted)	The phone number formatted in the international dialing code. N/A if not formattable.
Local Format (local_format)	The phone number formatted in the countrys local routing rules with area code. N/A if not formattable.
Valid (valid)	Is the phone number properly formatted and considered valid based on assigned phone numbers available to carriers in that country?
Fraud Score (fraud_score)	The IPQS risk score which estimates how likely a phone number is to be fraudulent. Scores 85+ are risky while Fraud Scores 90+ are high risk.
Recent Abuse (recent_abuse)	Has this phone number been associated with recent or ongoing fraud?
VOIP (VOIP)	Is this phone number a Voice Over Internet Protocol (VOIP) or digital phone number?
Prepaid (prepaid)	Is this phone number associated with a prepaid service plan?
Risky (risky)	Is this phone number associated with fraudulent activity, scams, robo calls, fake accounts, or other unfriendly behavior?
Carrier (carrier)	The carrier (service provider) this phone number has been assigned to or N/Aif unknown.
Line Type (line_type)	The type of line this phone number is associated with (Toll Free, Mobile, Landline, Satellite, VOIP, Premium Rate, Pager, etc...) or N/Aif unknown.
Country (country)	The two character country code for this phone number.
City (city)	City of the phone number if available or N/A if unknown.
Zip Code (zip_code)	Zip or Postal code of the phone number if available or N/A if unknown.
Region (region)	Region (state) of the phone number if available or N/A if unknown.
Dialing code (dialing_code)	The 1 to 4 digit dialing code for this phone number or null if unknown.
Active Status (active_status)	Additional details on the status of the subscriber connection when enhanced active line checks are enabled. Contact your account manager to enable this add-on feature. These values can be Active Line, Disconnected Line, Phone Turned Off, Inconclusive Status, or N/A if unknown.
Status of associated email address (associated_email_addresses.status)	The status of associated emails
Associated Emails (associated_email_addresses.emails)	A list with associated emails
User Activity (user_activity)	Frequency at which this phone number makes legitimate purchases, account registrations, and engages in legitimate user behavior online. Values can be high, medium, low, or none. Values of high or medium are strong signals of healthy usage. New phone numbers without a history of legitimate behavior will have a value as none
Mobile Network Code (mnc)	The Mobile Network Code(MNC) is a concise identifier that represents a specific mobile carrier or network within a given country. It helps quickly identify the mobile service provider associated with a mobile device, enabling efficient routing of communication and services
Mobile Country Code (mcc)	The Mobile Country Code is a numerical identifier that succinctly represents the specific country associated with a mobile phones network. This code helps in identifying the nation where the mobile device is registered or operational, facilitating accurate routing of mobile communications and services

Outputs	Description
Leaked (leaked)	Has this phone number recently been exposed in an online database breach or act of compromise
Spammer (spammer)	Indicates if the phone number has recently been reported for spam or harassing calls/texts
Do not call (do_not_call)	Indicates if the phone number is listed on any Do Not Call (DNC) lists. Only supported in US and CA. This data may not be 100% up to date with the latest DNC blacklists. Contact your account manager to enable better DNC data and TCPA litigator removal

IP Quality Score /Malicious URL Scanner method

Scans links in real-time to detect suspicious URL.

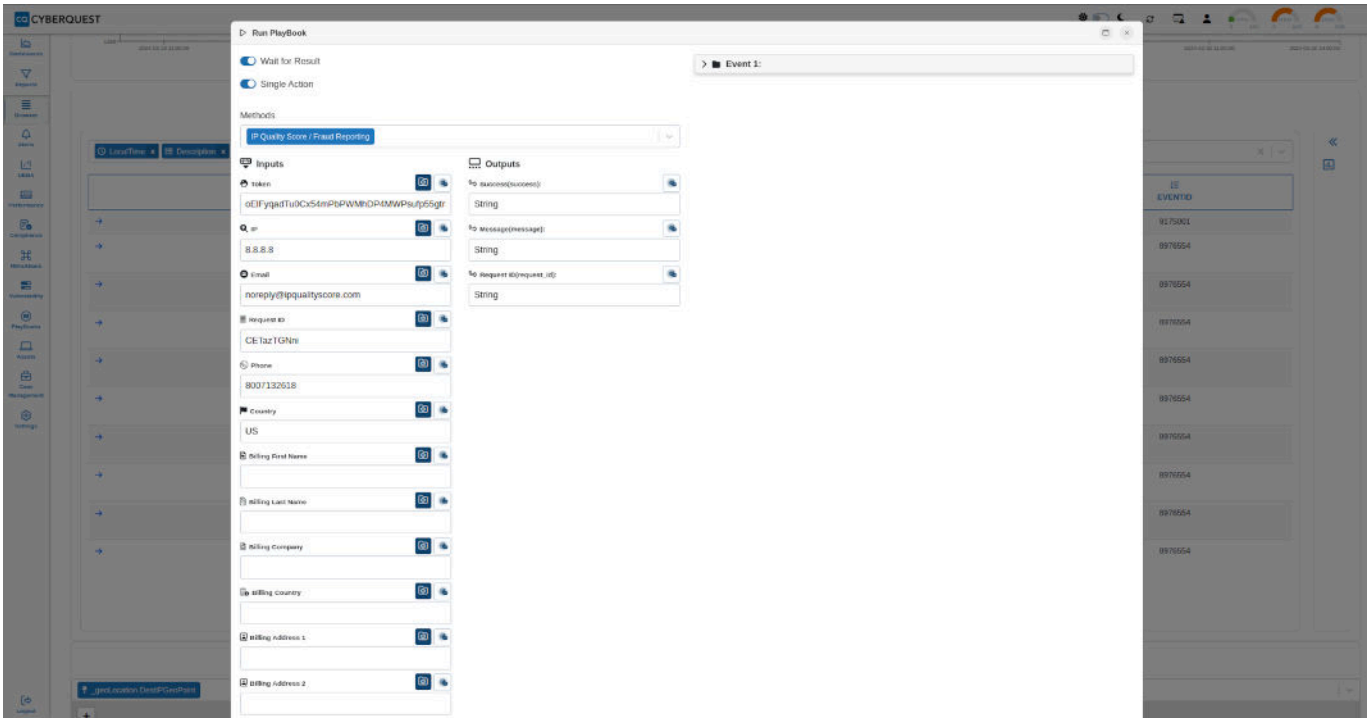


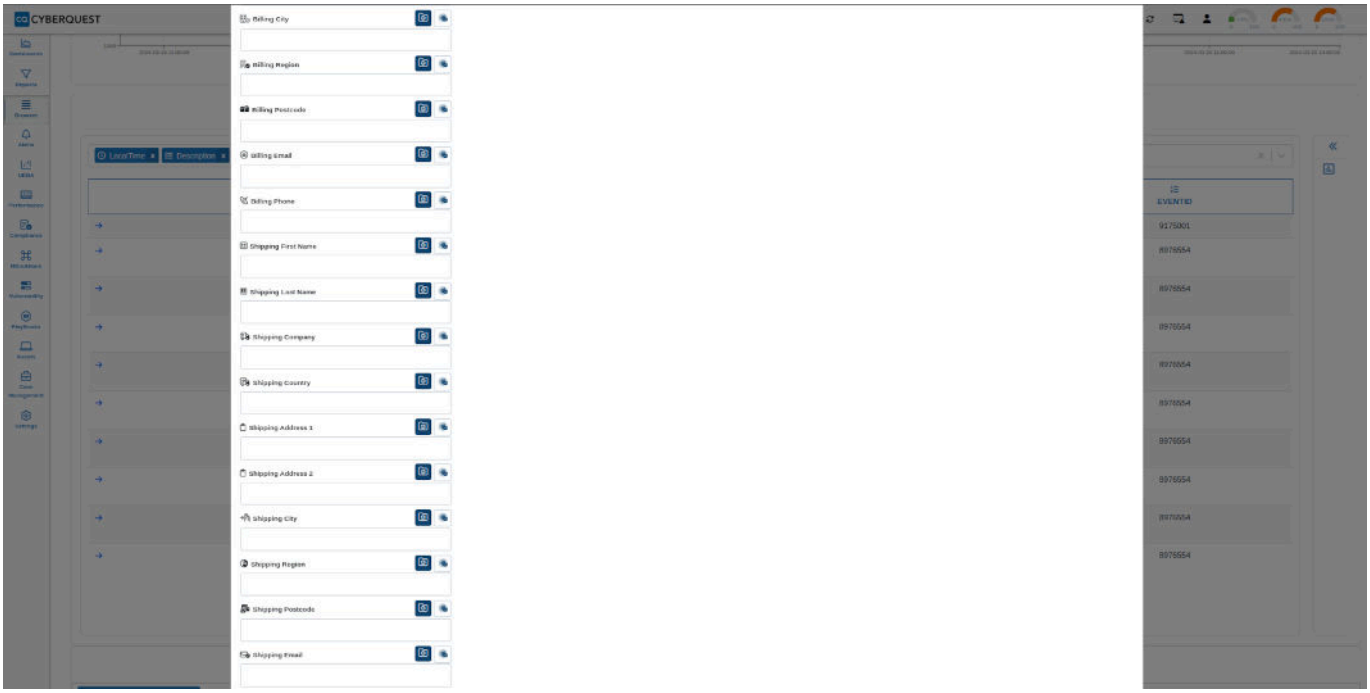
Inputs	Description
Token (is required)	To use IP Quality Score you need to have an API Key
URL (is required)	The URL which will be investigated
Fast	When this parameter is enabled our API will not perform an SMTP check with the mail service provider, which greatly increases the API speed. Syntax and DNS checks are still performed on the email address as well as our disposable email detection service. This option is intended for services that require decision making in a time sensitive manner.
Timeout	Maximum number of seconds to perform live page scanning and follow redirects. If your implementation requirements do not need an immediate response, we recommend bumping this value to 5. Default value is 2 seconds.
Strictness	How strict should we scan this URL? Stricter checks may provide a higher false-positive rate. We recommend defaulting to level 0, the lowest strictness setting, and increasing to 1 or 2 depending on your levels of abuse.

Outputs	Description
Success (success)	Was the request successful?
Message (message)	A generic status message, either success or some form of an error notice.
Unsafe (unsafe)	Is this domain suspected of being unsafe due to phishing, malware, spamming, or abusive behavior? View the confidence level by analyzing the Risk Score.
Domain (domain)	Domain name of the final destination URL of the scanned link, after following all redirects.
IP Address (ip_address)	The IP address corresponding to the server of the domain name.
Server (server)	The server banner of the domains IP address. For example: nginx/1.16.0. Value will be N/A if unavailable.
Content Type (content_type)	MIME type of URLs content. For example text/html; charset=UTF-8. Value will be N/A if unavailable.
Domain Rank (domain_rank)	Estimated popularity rank of website globally. Value is 0 if the domain is unranked or has low traffic.
DNS Valid (dns_valid)	The domain of the URL has valid DNS records.
Parking (parking)	Is the domain of this URL currently parked with a for sale notice?
Spamming (spamming)	Is the domain of this URL associated with email SPAM or abusive email addresses?
Malware (malware)	Is this URL associated with malware or viruses?
Phishing (phishing)	Is this URL associated with malicious phishing behavior?
Suspicious (suspicious)	Is this URL suspected of being malicious or used for phishing or abuse? Use in conjunction with the risk_score as a confidence level.
Adult (adult)	Is this URL or domain hosting dating or adult content?
Risk Score (risk_score)	The IPQS risk score which estimates the confidence level for malicious URL detection. Risk Scores 85+ are high risk, while Risk Scores = 100 are confirmed as accurate.
Country Code (country_code)	The country corresponding to the servers IP address.
Category (category)	Website classification and category related to the content and industry of the site. Over 70 categories are available including Video Streaming, Trackers, Gaming, Privacy, Advertising, Hacking, Malicious, Phishing, etc. The value will be N/A if unknown.
Domain Age in human readable format (domain_age_human)	A human description of when this domain was registered. (Ex: 3 months ago)
Domain Age Timestamp (domain_age_timestamp)	The unix time since epoch when this domain was first registered. (Ex: 1568061634)
Redirected (redirected)	Does the URL redirect to another domain when loaded in a browser?

IP Quality Score /Fraud Reporting method

List the syslog servers for a network.






shipping phone
username
Password Hash
Credit Card Bin
Credit Card Hash
Credit Card Expiration Month
credit card expiration year
Cancel
Run
EVENTID

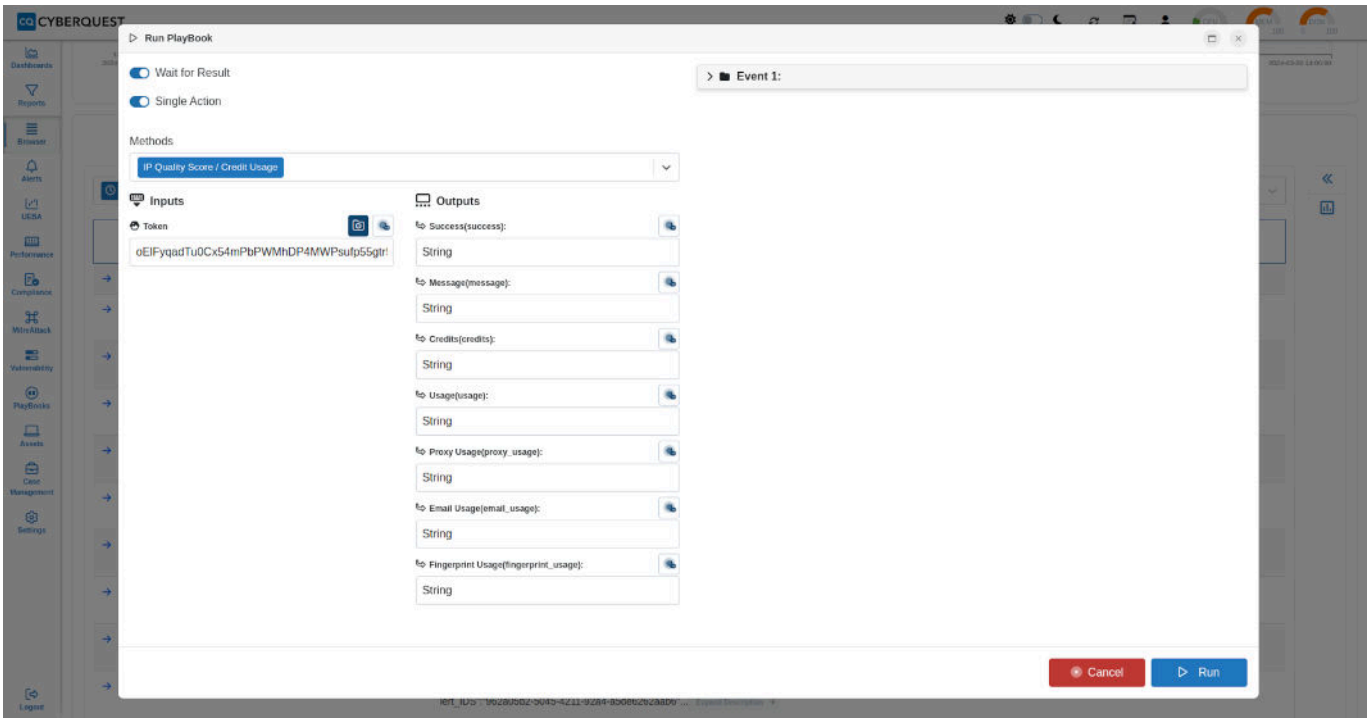
Inputs	Description
Token (is required)	To use IP Quality Score you need to have an API Key
IP	The IPv4 or IPv6 address you wish to report. (optional, one required)
Email	The email address you wish to report. (optional, one required)
Request ID	The Request ID you wish to report. (optional, one required)
Phone	The 9 to 20 digit phone number you wish to report. Must include country field below.(optional, one required, required with country below)
Country	The 2 letter country code (preferred method) or full properly formatted name (capitalization and spacing required) of the phone number you wish to report. Must include phone field above.(optional, one required, required with phone above)
Billing First Name	The customers billing first name.
Billing Last Name	The customers billing last name.
Billing Company	The customers billing company.
Billing Country	The customers billing country name or billing country ISO-Alpha2. (EG: United States or US)
Billing Address 1	The customers billing street address part 1.
Billing Address 2	The customers billing street address part 2.
Billing City	The customers billing city.
Billing Region	The customers billing region or state.
Billing Postcode	The customers billing postcode or zipcode.
Billing Email	The customers billing email address.
Billing Phone	The customers billing 11 to 14 digit phone number. (If less than 10 digits provided, the country code will be guessed by IP Quality Score AI.)
Shipping First Name	The customers shipping first name.
Shipping Last Name	The customers shipping last name.
Shipping Company	The customers shipping company.
Shipping Country	The customers shipping country name or shipping country ISO-Alpha2. (EG: United States or US)
Shipping Address 1	The customers shipping street address part 1.
Shipping Address 2	The customers shipping street address part 2.
Shipping City	The customers shipping city.
Shipping Region	The customers shipping region or state.
Shipping Postcode	The customers shipping postcode or zipcode.
Shipping Email	The customers shipping email address.
Shipping Phone	The customers shipping phone number
Username	The customers username.
Password Hash	For security reasons and following industry best practices, a SHA256 hash of the users password for better user analysis.
Credit Card Bin	First six digits of the credit or debit card, referred to ask the Bank Identification Number.

Inputs	Description
Credit Card Hash	For security reasons and following industry best practices, a SHA256 hash of the credit card number is accepted to check against blacklisted cards.
Credit Card Expiration Month	Two letter format of the credit cards expiration month. For example, May would be 05.
Credit Card Expiration Year	Two letter format of the credit cards expiration year. For example, 2023 would be 23.
AVS Code	One letter Address Verification Service (AVS) response code provided by the credit card processor or bank.
CVV Code	One letter Card Verification Value (CVV2) response code provided by the credit card processor or bank.
Order Amount	Total balance of the entire order without currency symbols.
Order Quantity	Quantity of items for this order.
Recurring	Is this a recurring order that automatically rebills?
Recurring Times	If this is a recurring order, then how many times has this recurring order rebilled? For example, if this is the third time the user is being billed, please enter this value as 3. If this is the initial recurring order, please leave the value as blank or enter 1.

Outputs	Description
Success (success)	Was the request successful?
Message (message)	A generic status message, either success or some form of an error notice.
Request ID (request_id)	A unique identifier for this request that can be used to lookup the request details or send a postback conversion notice.

IP Quality Score /Credit Usage method

Access your accounts total number of available credits and current usage for this billing period.



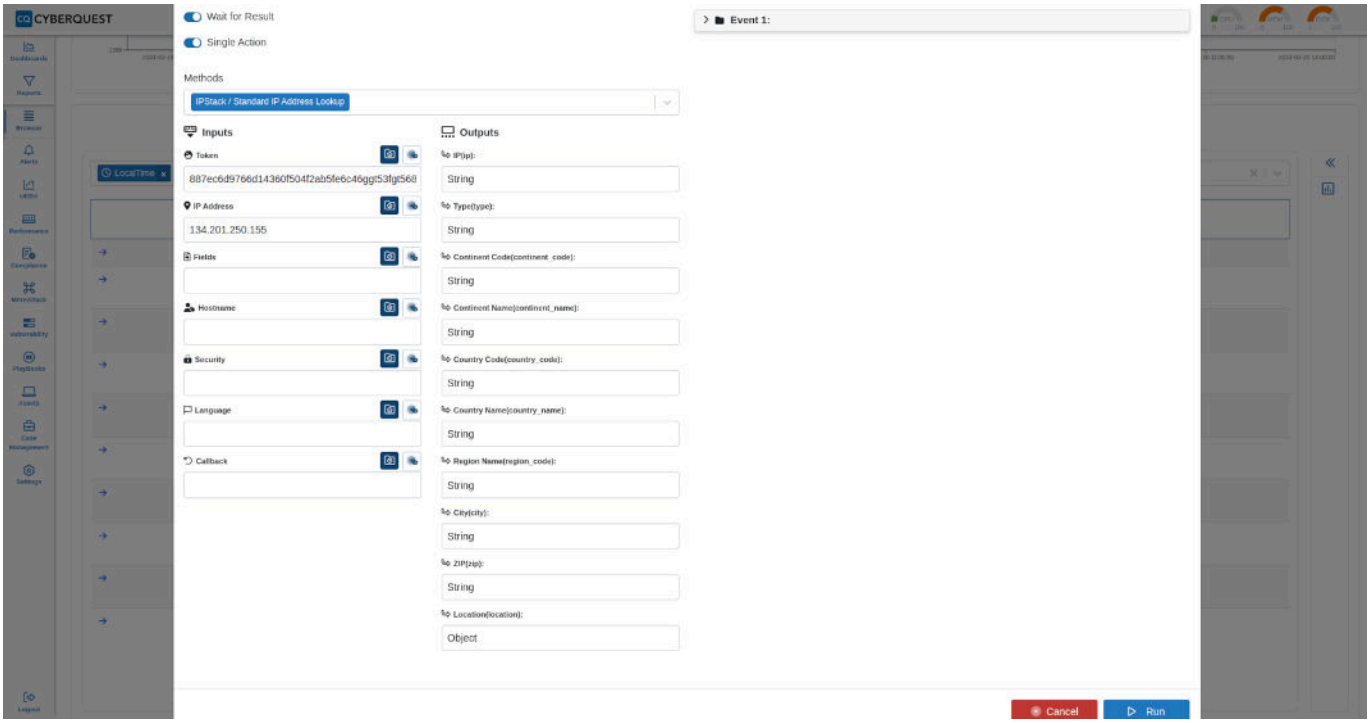
Inputs	Description
Token (is required)	To use IP Quality Score you need to have an API KeyTo use IP Quality Score you need to have an API Key

Outputs	Description
Success (success)	Was the request successful?
Message (message)	A generic status message, either success or some form of an error notice.
Credits (credits)	The remaining credits on the API Key
Usage (usage)	How many times were used the APIs calls
Proxy Usage (proxy_usage)	How many times was used proxy api
Email Usage (email_usage)	How many times was used email usage
Fingerprint Usage (fingerprint_usage)	How many times was used fingerprint usage

IPStack

IPStack/Standard IP Address Lookup method

Standard Lookup is used to look up single IPv4 or IPv6 addresses.

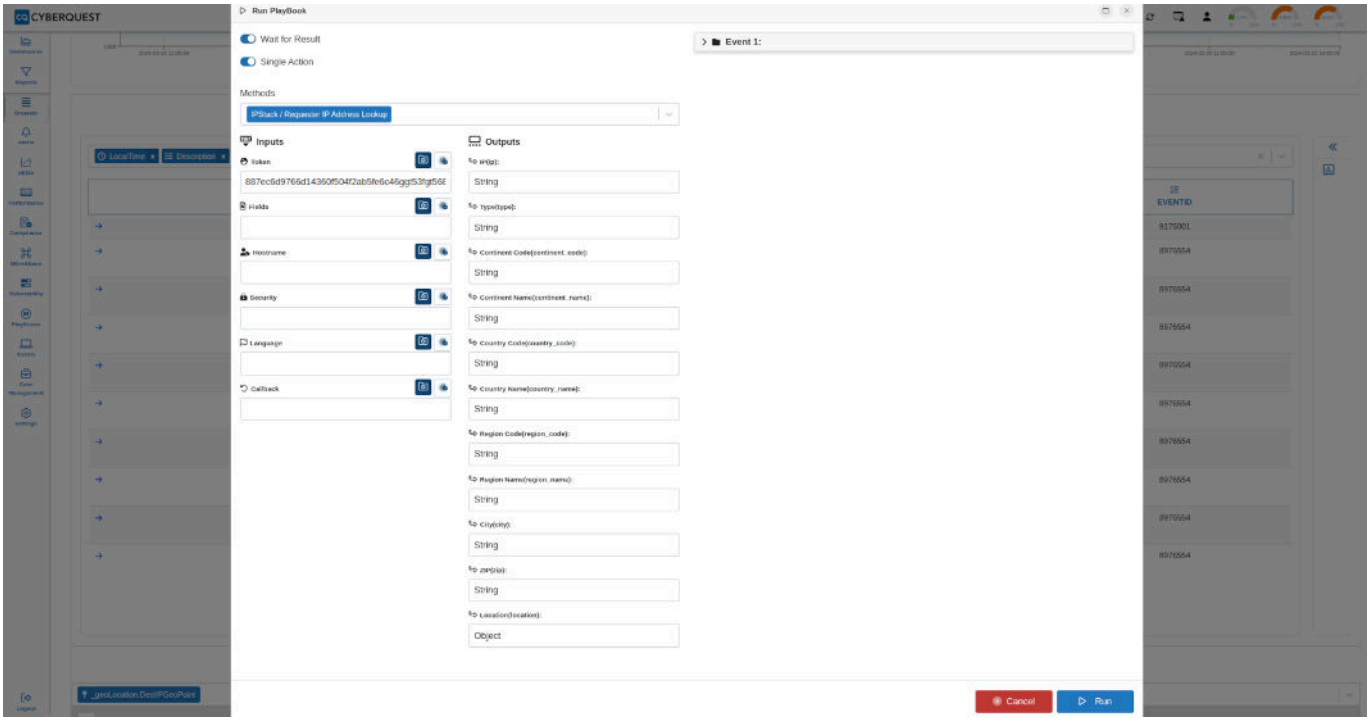


Inputs	Description
Token (is required)	To use the IPStack API, you must have an API key.
IP Address (is required)	Any IPv4 or IPv6 address; you can also enter a domain URL to have ipstack resolve the domain to the underlying IP address.
Fields	Set to your preferred output field(s) according to the Specify Output Fields section.
Hostname	Set to 1 to enable Hostname Lookup.
Security	Set to 1 to enable the Security module.
Language	Set to a 2-letter language code according to the Specify Output Language section to change output language.
Callback	Specify a JSONP callback function name according to the JSONP Callbacks section.

Outputs	Description
IP (ip)	Returns the requested IP address
Type (type)	Returns the IP address type IPv4 or IPv6
Continent Code (continent_code)	Returns the 2-letter country code associated with the IP
Continent Name (continent_name)	Returns the name of the country associated with the IP
Country Code (country_code)	Returns the 2-letter country code associated with the IP
Country Name (country_name)	Returns the name of the country associated with the IP
Region Name (region_code)	Returns the region code of the region associated with the IP (e.g. CA for California)
City (city)	Returns the name of the city associated with the IP
ZIP (zip)	Returns the ZIP code associated with the IP
Location (location)	Returns multiple location-related objects

IPStack/Requester IP Address Lookup method

Look up for the IP from which the request comes.



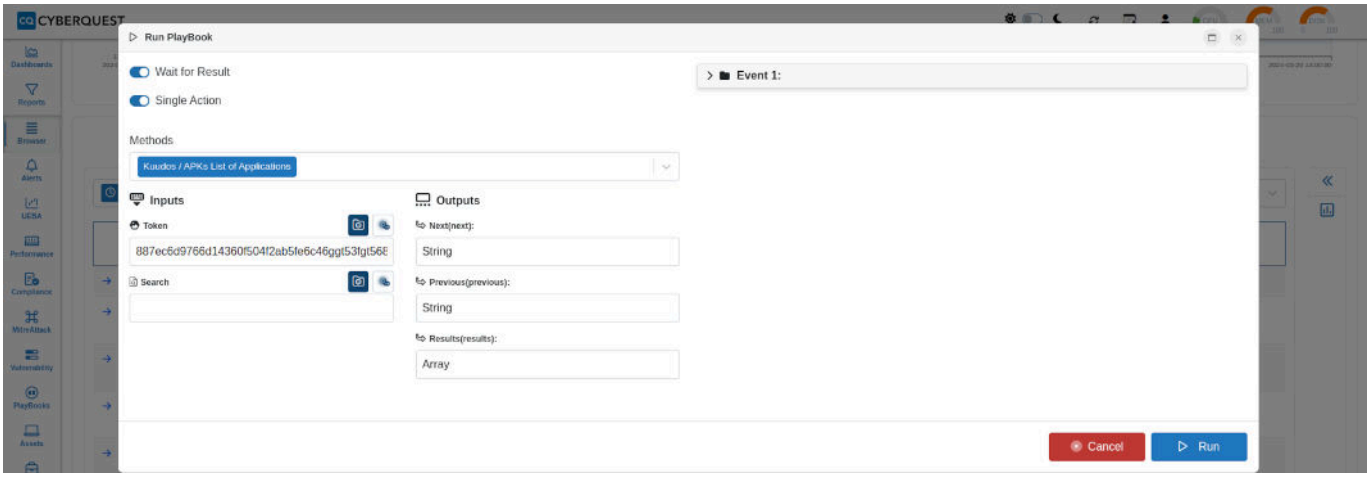
Inputs	Description
Token (is required)	To use the IPStack API, you must have an API key.
Fields	Set to your preferred output field(s) according to the Specify Output Fields section.
Hostname	Set to 1 to enable Hostname Lookup.
Security	Set to 1 to enable the Security module.
Language	Set to a 2-letter language code according to the Specify Output Language section to change output language.
Callback	Specify a JSONP callback function name according to the JSONP Callbacks section.

Outputs	Description
IP (ip)	Returns the requested IP address
Type (type)	Returns the IP address type IPv4 or IPv6
Continent Code (continent_code)	Returns the 2-letter country code associated with the IP
Continent Name (continent_name)	Returns the name of the country associated with the IP
Country Code (country_code)	Returns the 2-letter country code associated with the IP
Country Name (country_name)	Returns the name of the country associated with the IP
Region Code (region_code)	Returns the region code of the region associated with the IP (e.g. CA for California)
Region Name (region_name)	Returns the name of the region associated with the IP
City (city)	Returns the name of the city associated with the IP
ZIP (zip)	Returns the ZIP code associated with the IP
Location (location)	Returns multiple location-related objects

Kuudos

Kuudos/APKs List of Applications method

List of applications (APKs).

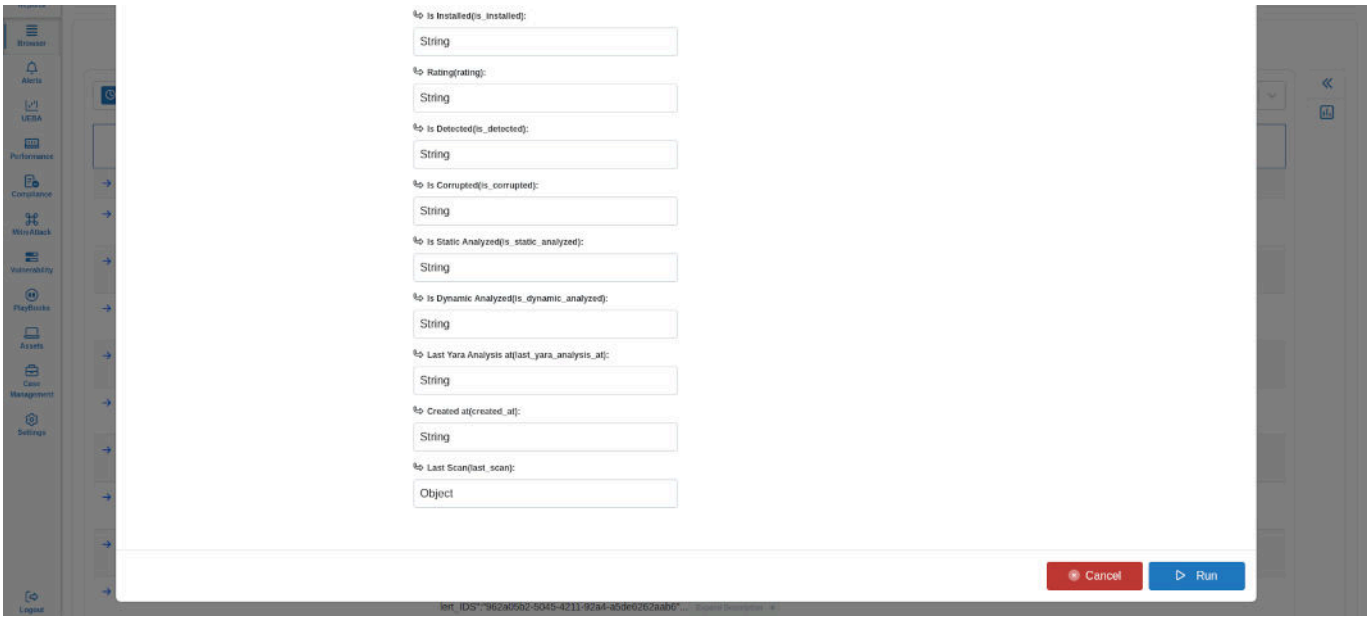


Inputs	Description
Token (is required)	To use the Kuudos API, you must have an API key.
Search	Allow advanced search.

Outputs	Description
Next (next)	URL to the next page
Previous (previous)	URL to the previous page
Results (results)	The results of the API call

Kuudos/Detailed Information about an APK method

An APKs detailed information.

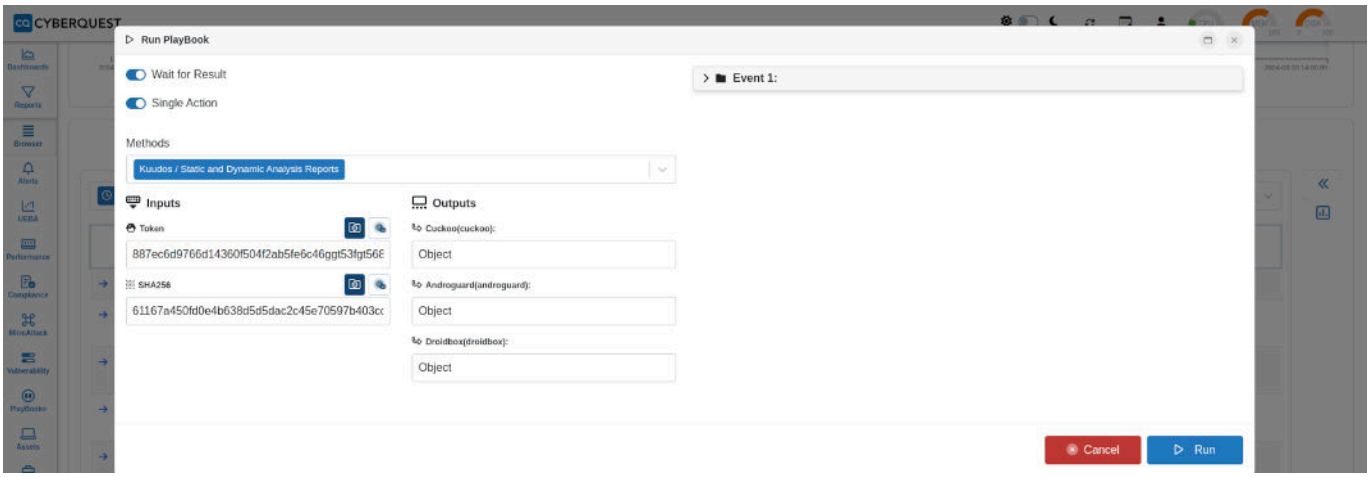


Inputs	Description
Token (is required)	To use the Kuudos API, you must have an API key.
SHA256 (is required)	Identify APK based on sha256

Outputs	Description
ID (id)	The ID of the investigated APK SHA
URL (url)	The URL of the investigated APK
SHA256 (sha256)	The SHA256 of the investigated APK
MD5 (md5)	The MD5 of the investigated APK
SHA1 (sha1)	The SHA1 of the investigated APK
APP (app)	The name of the investigated APK
Package Name (package_name)	The package name of the investigated APK
Company (company)	The OS where the APK can be installed
Is trusted (is_trusted)	True if the app is not a malware, otherwise false
Is Installed (is_installed)	True if the app is installed, otherwise false
Rating (rating)	The value assigned by Koodous
Is Detected (is_detected)	True if the APK is detected, otherwise false
Is Corrupted (is_corrupted)	True if the APK is detected, otherwise false
Is Static Analyzed (is_static_analyzed)	True if the APK is static analyzed, otherwise false
Is Dynamic Analyzed (is_dynamic_analyzed)	True if the APK is static analyzed, otherwise false
Last Yara Analysis at (last_yara_analysis_at)	The results of the last Yara Analysis
Created at (created_at)	The timestamp when report was created
Last Scan (last_scan)	The results of the last scan

Kuudos/Static and Dynamic Analysis Reports method

Get a copy of the static and dynamic analysis reports.



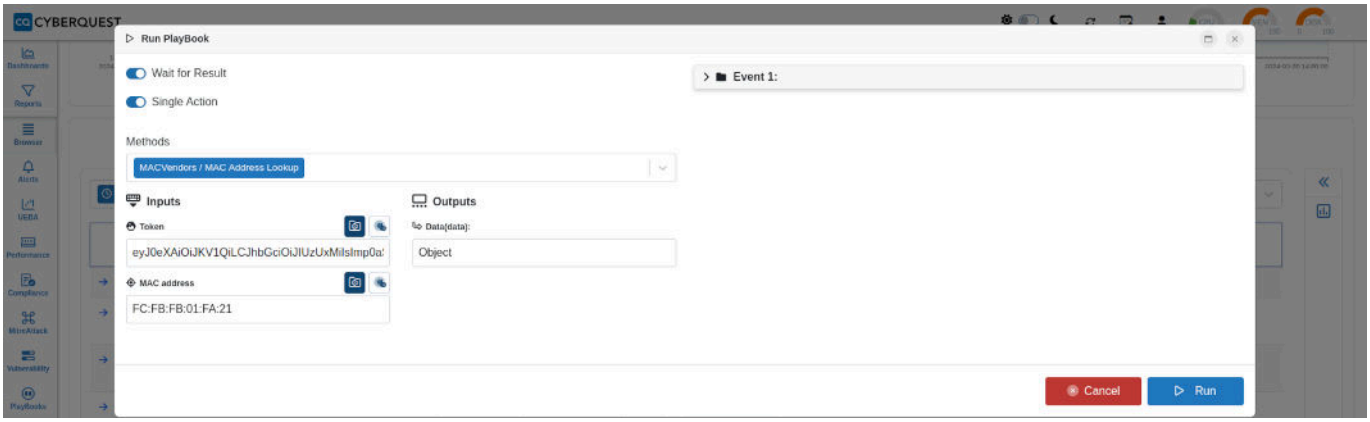
Inputs	Description
Token	To use the Kuudos API, you must have an API key.
SHA256 (is required)	Identify APK based on sha256

Outputs	Description
Cuckoo (cuckoo)	The results from Cuckoo
Androguard (androguard)	The results from Androguard
Droidbox (droidbox)	The results from Droidbox

MacVendors

MACVendors /MAC Address Lookup method

This API performs a quick and easy vendor lookup for mac addresses.



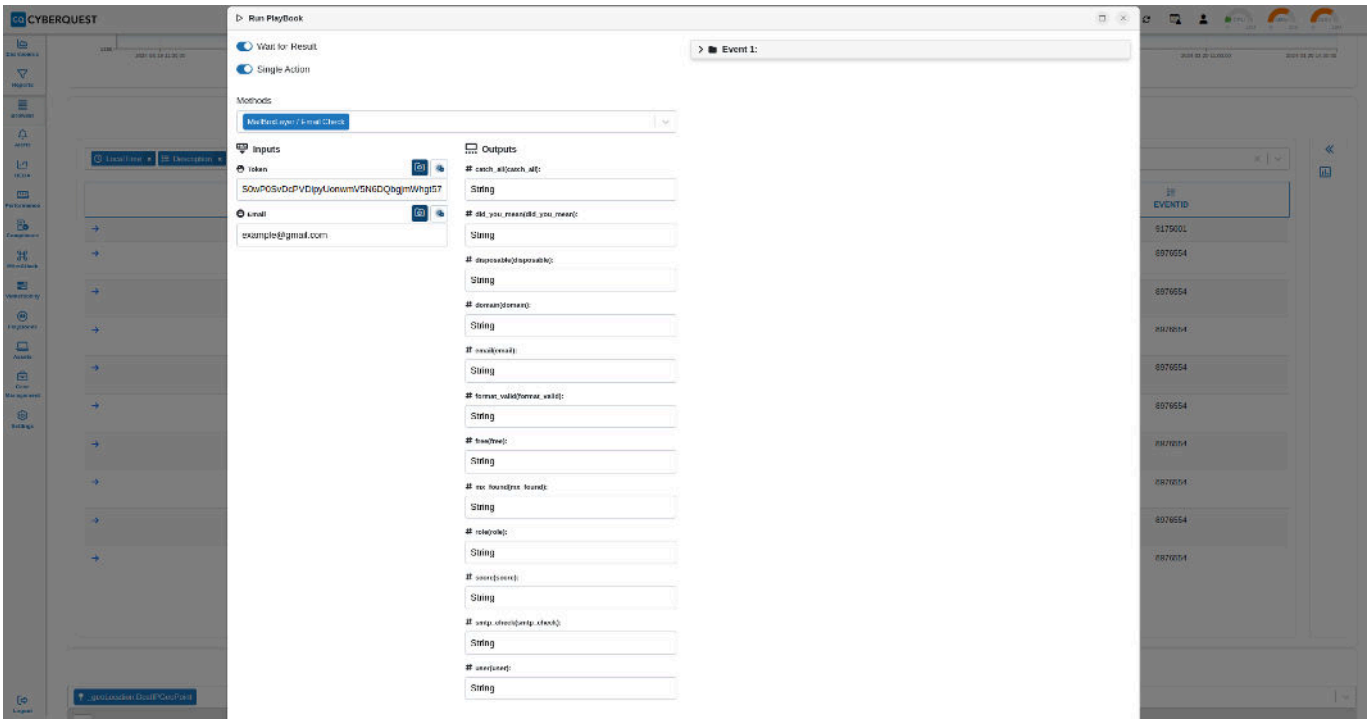
Inputs	Description
Token (is required)	To use the MacVendors API, you must have an API key.
MAC address (is required)	The MAC address that is being searched.

Outputs	Description
Data (data)	The results of the API call

Mailboxlayer

MailBoxLayer/Email Check method

Validates and verifies an email address in order to determine deliverability and quality.

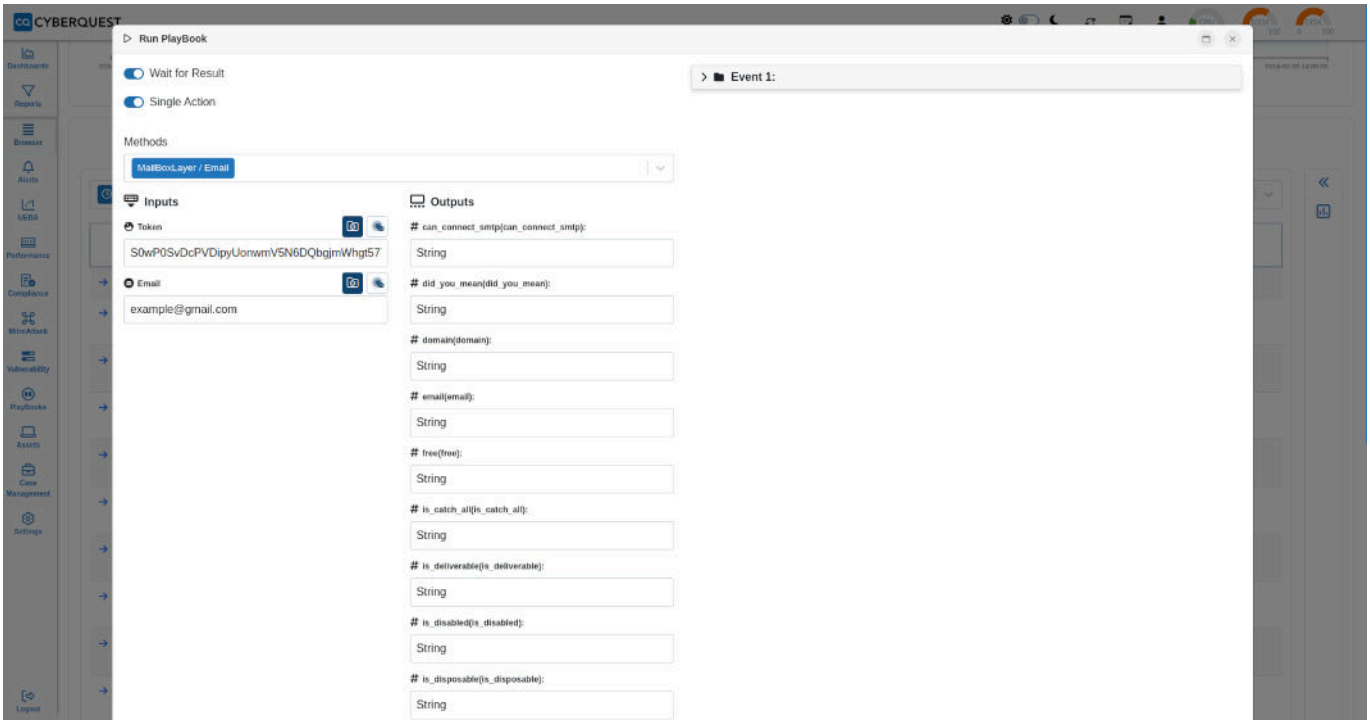


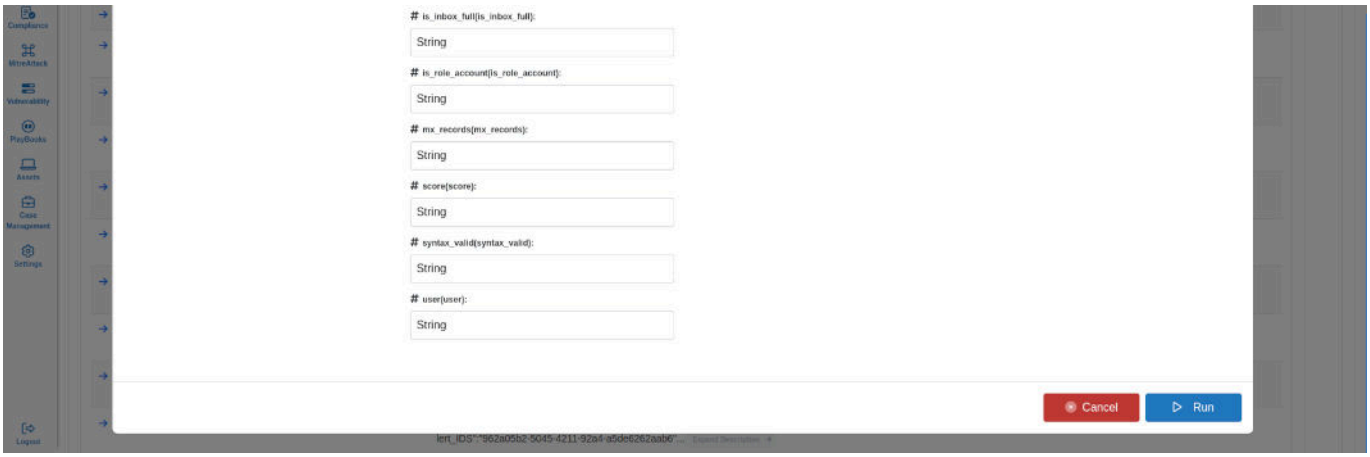
Inputs	Description
Token (is required)	To use the Mailboxlayer API, you must have an API key.
Email (is required)	Email to check

Outputs	Description
catch_all (catch_all)	Returns true or false depending on whether or not the requested email address is found to be part of a catch-all mailbox
did_you_mean (did_you_mean)	Contains a did-you-mean suggestion in case a potential typo has been detected
disposable (disposable)	Returns true or false depending on whether or not the requested email address is a disposable email address. (e.g. user123@mailinator.com) Returns true or false depending on whether or not the requested email address is a disposable email address. (e.g. user123@mailinator.com)
domain (domain)	Returns the domain of the requested email address. (e.g. company.com in paul@company.com)
email (email)	Contains the exact email address requested
format_valid (format_valid)	Returns true or false depending on whether or not the general syntax of the requested email address is valid
free (free)	Returns true or false depending on whether or not the requested email address is a free email address. (e.g. user123@gmail.com, user123@yahoo.com)
mx_found (mx_found)	Returns true or false depending on whether or not MX-Records for the requested domain could be found
role (role)	Returns true or false depending on whether or not the requested email address is a role email address. (e.g. support@company.com, postmaster@company.com)
score (score)	Returns a numeric score between 0 and 1 reflecting the quality and deliverability of the requested email address.
smtp_check (smtp_check)	Returns true or false depending on whether or not the SMTP check of the requested email address succeeded
user (user)	Returns the local part of the request email address. (e.g. paul in paul@company.com)

MailBoxLayer/Email method

Validates and verifies an email address in order to determine deliverability and quality.





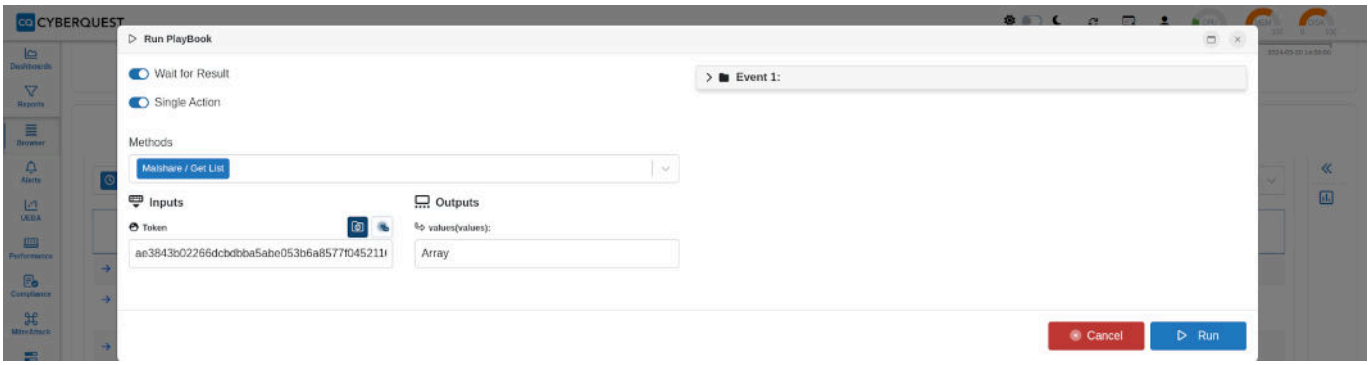
Inputs	Description
Token (is required)	To use the Mailboxlayer API, you must have an API key.
Email (is required)	Email to check

Outputs	Description
can_connect_smtp (can_connect_smtp)	True if it is possible to connect to SMTP
did_you_mean (did_you_mean)	Contains a did-you-mean suggestion in case a potential typo has been detected
domain (domain)	Returns the domain of the requested email address. (e.g. company.com in paul@company.com)
email (email)	Contains the exact email address requested
free (free)	Returns true or false depending on whether or not the requested email address is a free email address. (e.g. user123@gmail.com, user123@yahoo.com)
is_catch_all (is_catch_all)	Returns true or false depending on whether or not the requested email address is found to be part of a catch-all mailbox
is_deliverable (is_deliverable)	True if the email is deliverable, otherwise false
is_disabled (is_disabled)	True if the email is disabled, otherwise false
is_disposable (is_disposable)	True if the email is disposable, otherwise false
is_inbox_full (is_inbox_full)	True if the inbox is full, otherwise false
is_role_account (is_role_account)	True if it is role account, otherwise false
mx_records (mx_records)	True if it has MX Records
score (score)	Returns a numeric score between 0 and 1 reflecting the quality and deliverability of the requested email address
syntax_valid (syntax_valid)	True if the syntax of mail correct, otherwise false
user (user)	Returns the local part of the request email address. (e.g. paul in paul@company.com)

Malshare

Malshare/Get List method

List hashes from the past 24 hours in JSON Format.

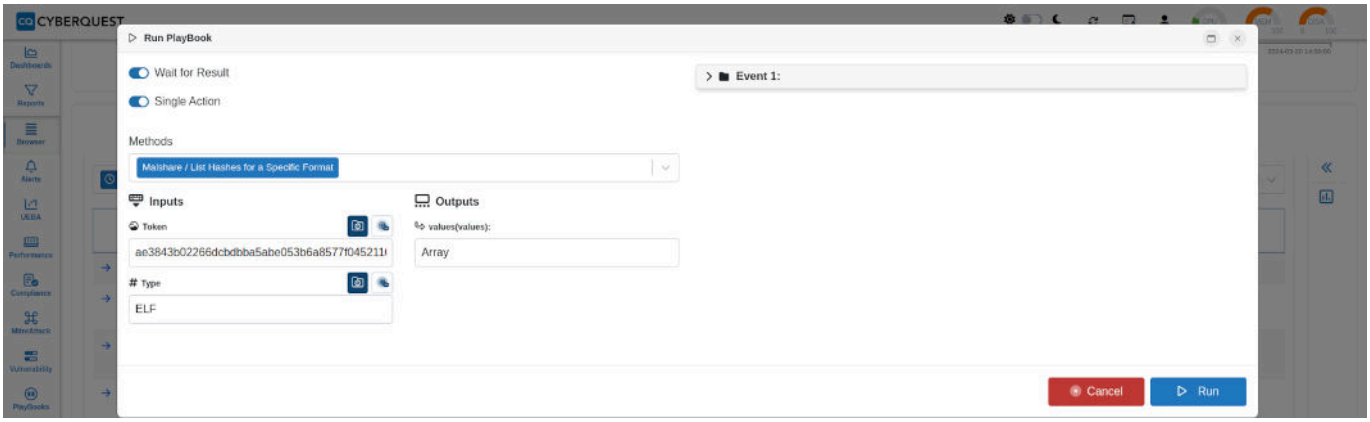


Inputs	Description
Token (is required)	To use the Malshare API, you must have an API key.

Outputs	Description
values (values)	The results of the API call

Malshare/List Hashes for a Specific Format method

List MD5/SHA1/SHA256 hashes of a specific type from the past 24 hours, in JSON format.

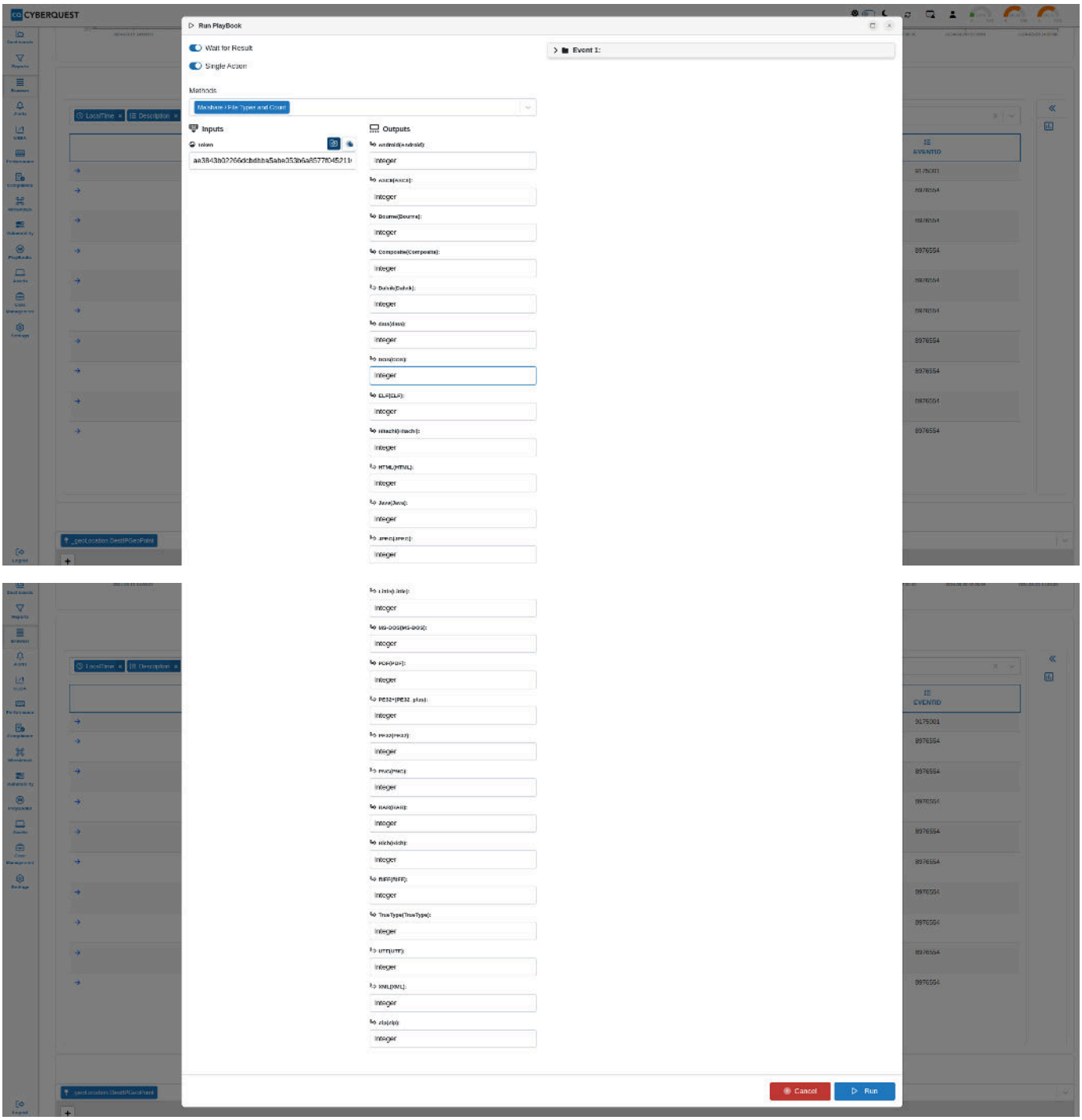


Inputs	Description
Token (is required)	To use the Malshare API, you must have an API key.
Type (is required)	Type of file

Outputs	Description
values (values)	The results of the API call

Malshare/File Types and Count method

Get list of file types & count from the past 24 hours, in JSON format.

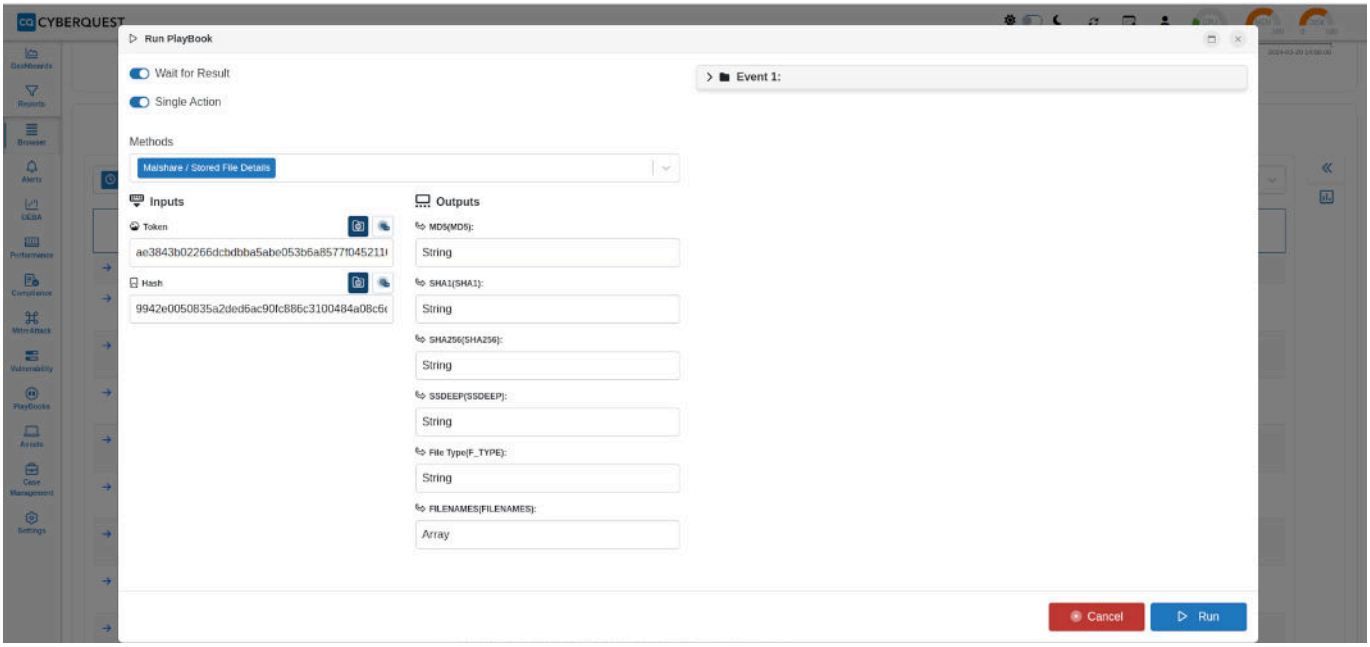


Inputs	Description
Token (is required)	To use the Malshare API, you must have an API key.

Outputs	Description
Android (Android)	The number of Android files detected in the last 24 hours
ASCII (ASCII)	The number of ASCII files detected in the last 24 hours
Bourne (Bourne)	The number of Bourne files detected in the last 24 hours
Composite (Composite)	The number of Composite files detected in the last 24 hours
Dalvik (Dalvik)	The number of Dalvik files detected in the last 24 hours
data (data)	The number of data files detected in the last 24 hours
DOS (DOS)	The number of DOS files detected in the last 24 hours
ELF (ELF)	The number of ELF files detected in the last 24 hours
Hitachi (Hitachi)	The number of Hitachi files detected in the last 24 hours
HTML (HTML)	The number of HTML files detected in the last 24 hours
Java (Java)	The number of Java files detected in the last 24 hours
JPEG (JPEG)	The number of JPEG files detected in the last 24 hours
Little (Little)	The number of Little files detected in the last 24 hours
MS-DOS (MS-DOS)	The number of MS-DOS files detected in the last 24 hours
PDF (PDF)	The number of PDF files detected in the last 24 hours
PE32+ (PE32_plus)	The number of PE32+ files detected in the last 24 hours
PE32 (PE32)	The number of PE32 files detected in the last 24 hours
PNG (PNG)	The number of PNG files detected in the last 24 hours
RAR (RAR)	The number of RAR files detected in the last 24 hours
Rich (Rich)	The number of RIFF files detected in the last 24 hours
RIFF (RIFF)	The number of RIFF files detected in the last 24 hours
TrueType (TrueType)	The number of TrueType files detected in the last 24 hours
UTF (UTF)	The number of UTF files detected in the last 24 hours
XML (XML)	The number of XML files detected in the last 24 hours
Zip (Zip)	The number of ZIP files detected in the last 24 hours

Malshare/Stored File Details method

Get stored file details in JSON format.

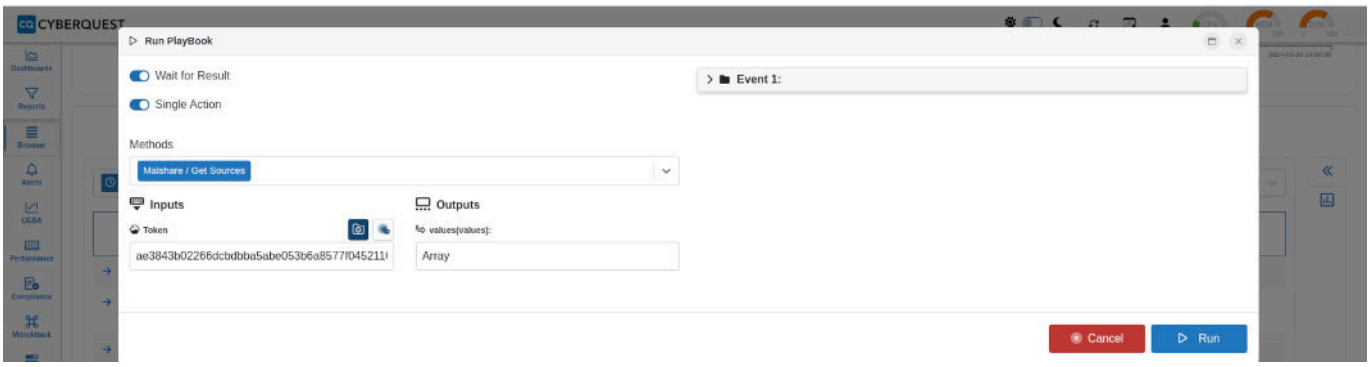


Inputs	Description
Token (is required)	To use the Malshare API, you must have an API key.
Hash (is required)	Identify file based on hash

Outputs	Description
MD5 (MD5)	MD5 of the file
SHA1 (SHA1)	SHA1 of the file
SHA256 (SHA256)	SHA256 of the file
SSDEEP (SSDEEP)	SSDEEP of the file
File Type (F_TYPE)	File Type of the file
FILENAMES (FILENAMES)	A list of filenames

Malshare/Get Sources method

List of sample sources from the past 24 hours, in JSON format.

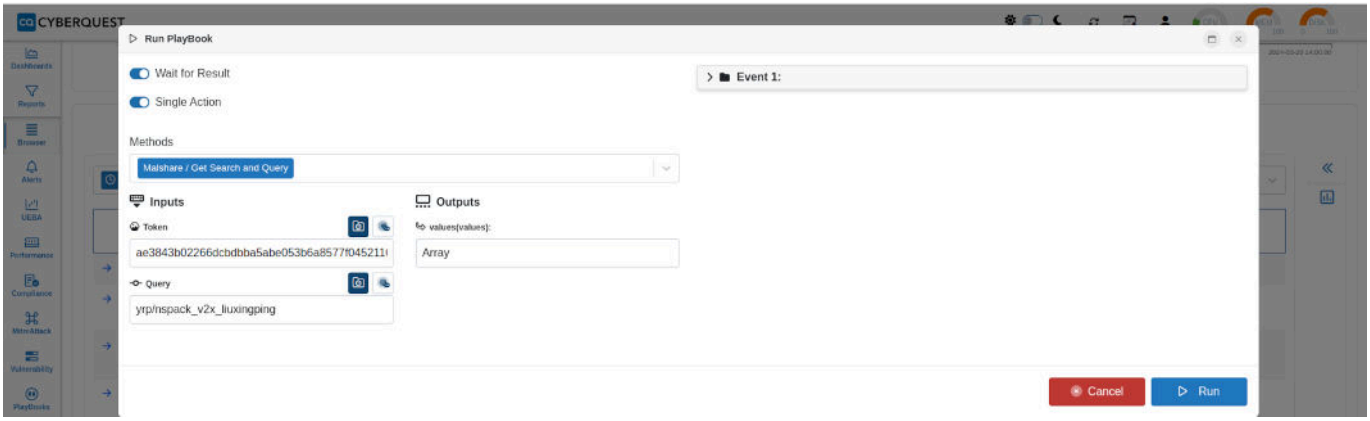


Inputs	Description
Token (is required)	To use the Malshare API, you must have an API key.

Outputs	Description
values (values)	The results of the API call

Malshare/Get Search and Query method

Search sample hashes, sources and file names in Raw data format.

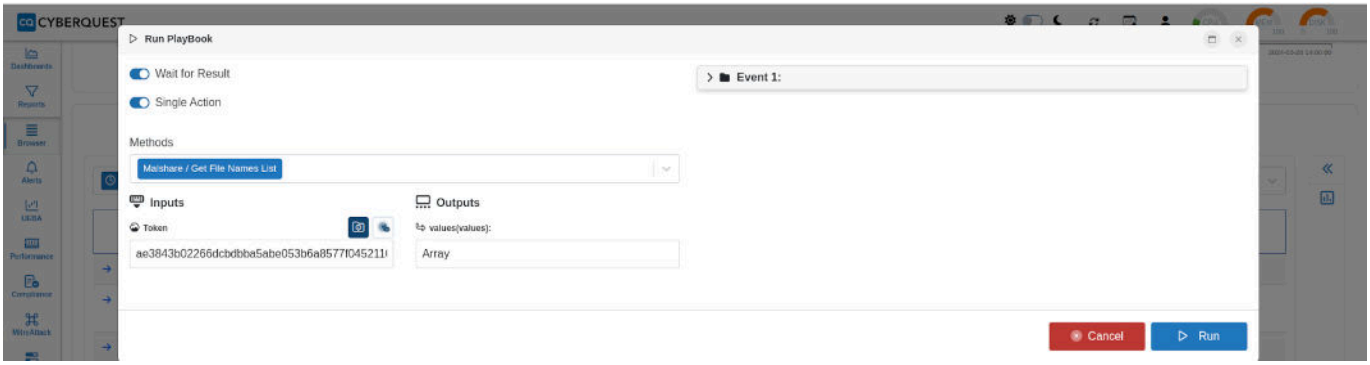


Inputs	Description
Token (is required)	To use the Malshare API, you must have an API key.
Query (is required)	Search query

Outputs	Description
values (values)	The results of the API call

Malshare/Get File Names List method

Returns a list of file names from recent uploads.



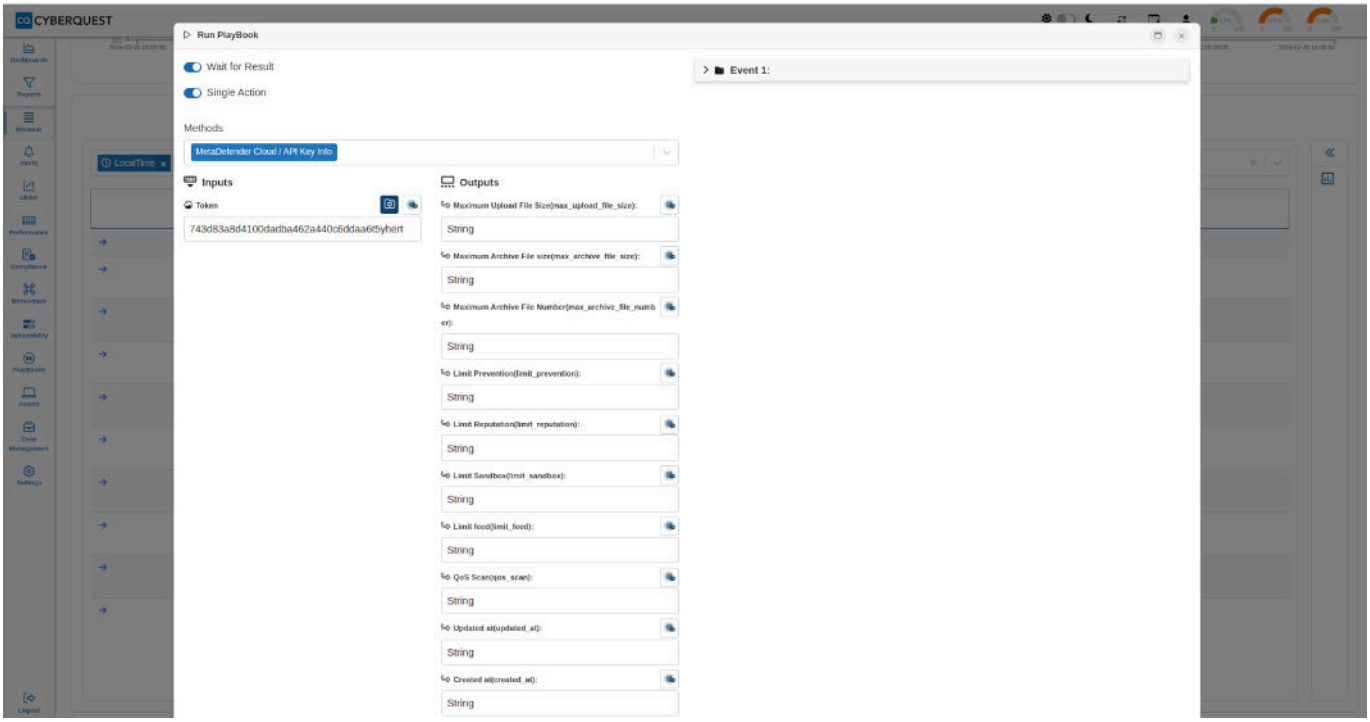
Inputs	Description
Token (is required)	To use the Malshare API, you must have an API key.

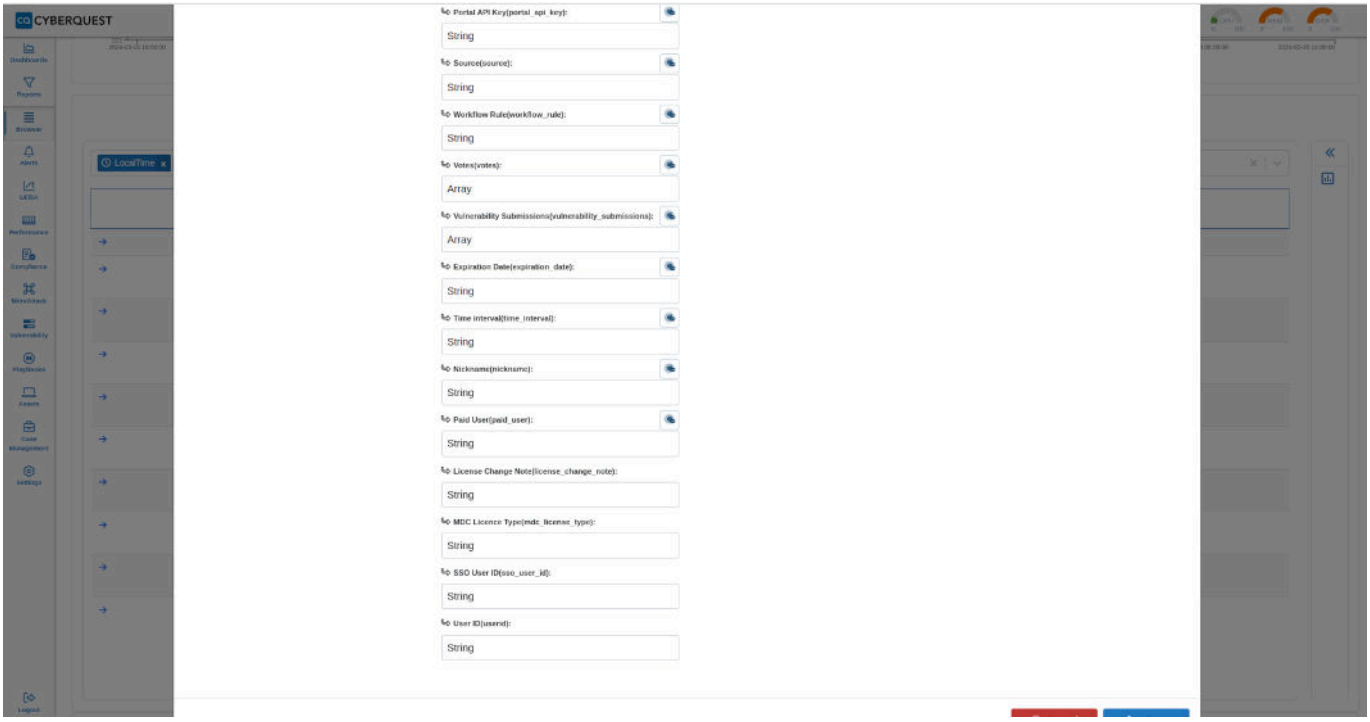
Outputs	Description
values (values)	The results of the API call

MetaDefender Cloud

MetaDefender Cloud/API Key Info method

Retrieve information about your apikey such as (but not limited to): max file size, API limits, created date, expiration date, and account nickname.



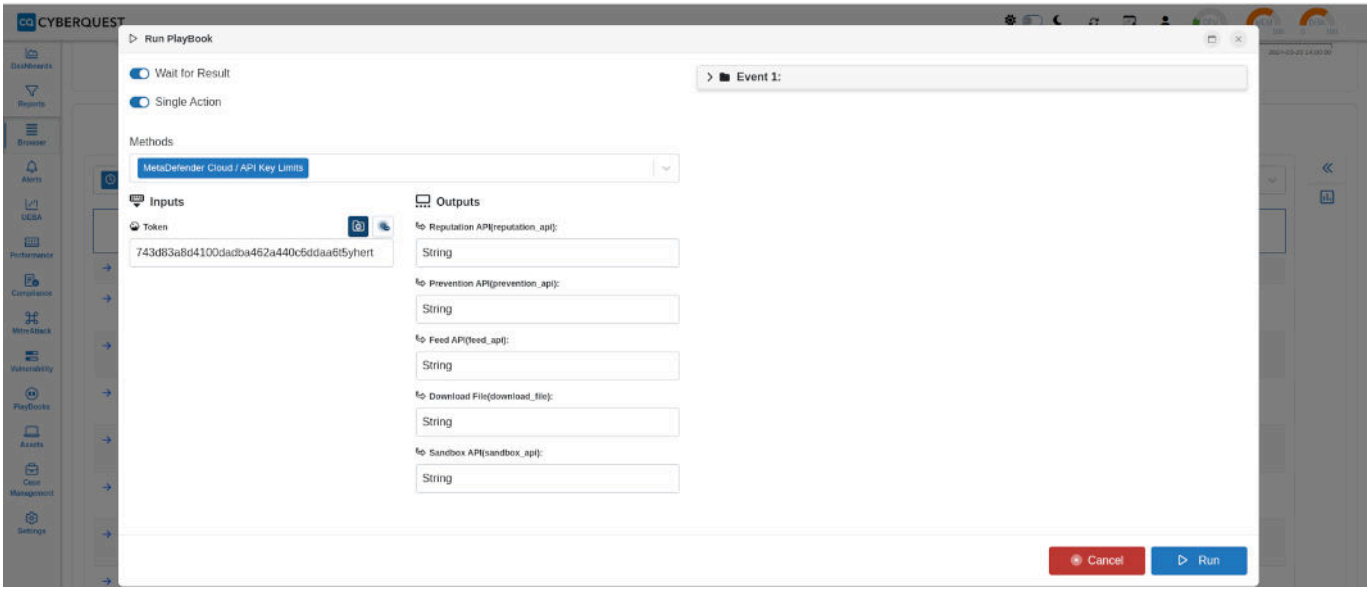


Inputs	Description
Token (is required)	To use the MetaDefenderCloud API, you must have an API key.

Outputs	Description
Maximum Upload File Size (max_upload_file_size)	The maximum upload size for files (expressed in MB)
Maximum Archive File size (max_archive_file_size)	The maximum upload size for archives (expressed in MB)
Maximum Archive File Number (max_archive_file_number)	The maximum number of files contained in an archive
Limit Prevention (limit_prevention)	The daily limit of Prevention API calls. The daily limit is reset 24 hours after the first call on a given day.
Limit Reputation (limit_reputation)	The daily limit of Reputation API calls. The daily limit is reset 24 hours after the first call on a given day.
Limit Sandbox (limit_sandbox)	The daily limit of Sandbox API calls. The daily limit is reset 24 hours after the first call on a given day.
Limit feed (limit_feed)	The daily limit of Feed API calls. The daily limit is reset 24 hours after the first call on a given day.
QoS Scan (qos_scan)	The selected scan queue, based on the apikey type
Updated at (updated_at)	The last date when the apikey information was updated
Created at (created_at)	The date when the apikey was created
Portal API Key (portal_api_key)	The apikey that has been queried
Source (source)	Provides information about the remaining usage limits for an API key. It indicates how many more API requests can be made using the specific API key, helping users manage their resource allocation effectively.
Workflow Rule (workflow_rule)	Signifies the defined set of rules or conditions that determine the workflow or sequence of actions that the API key is allowed to perform. This parameter helps manage and control the usage of the API key by specifying the specific actions, restrictions, or processes that can be executed within the given limits.
Votes (votes)	Refers to the count or allowance of votes that a user or API key has for certain actions or decisions within the platform.
Vulnerability Submissions (vulnerability_submissions)	Number of vulnerability submissions done by the user correlated to the queried apikey
Expiration Date (expiration_date)	The expiration date of the apikey. For paid apikeys this date is in the future.
Time interval (time_interval)	The duration of time your apikey limit lasts for (daily for most)
Nickname (nickname)	The nickname of the user correlated to the queried apikey
Paid User (paid_user)	This parameter helps distinguish between paid and free users, potentially affecting usage limits, features, or privileges within the API based on the subscription level.
License Change Note (license_change_note)	Informations about the licenses changes
MDC Licence Type (mdc_license_type)	Informations about the Modification Detection Code license
SSO User ID (sso_user_id)	The SSO user id corresponding to the apikey
User ID (userid)	The userid corresponding to the apikey

MetaDefender Cloud/API Key Limits method

Retrieve information about the consumed limits for an apikey.

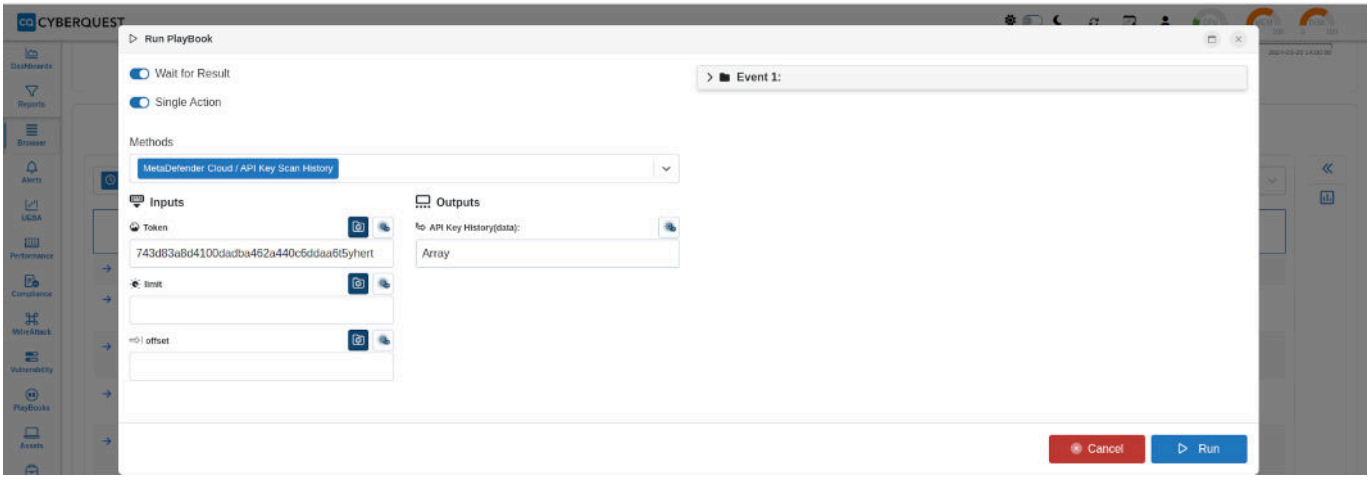


Inputs	Description
Token (is required)	To use the MetaDefenderCloud API, you must have an API key.

Outputs	Description
Reputation API (reputation_api)	The consumed Reputation API limits for the apikey
Prevention API (prevention_api)	The consumed Prevention API limits for the apikey
Feed API (feed_api)	The consumed Feed API limits for the apikey
Download File (download_file)	The consumed limits for file downloads for the apikey
Sandbox API (sandbox_api)	The consumed Dynamic Analysis API limits for the apikey

MetaDefender Cloud/API Key Scan History method

Retrieve a paginated list of files uploaded by the user in reverse chronological order (newest to oldest).

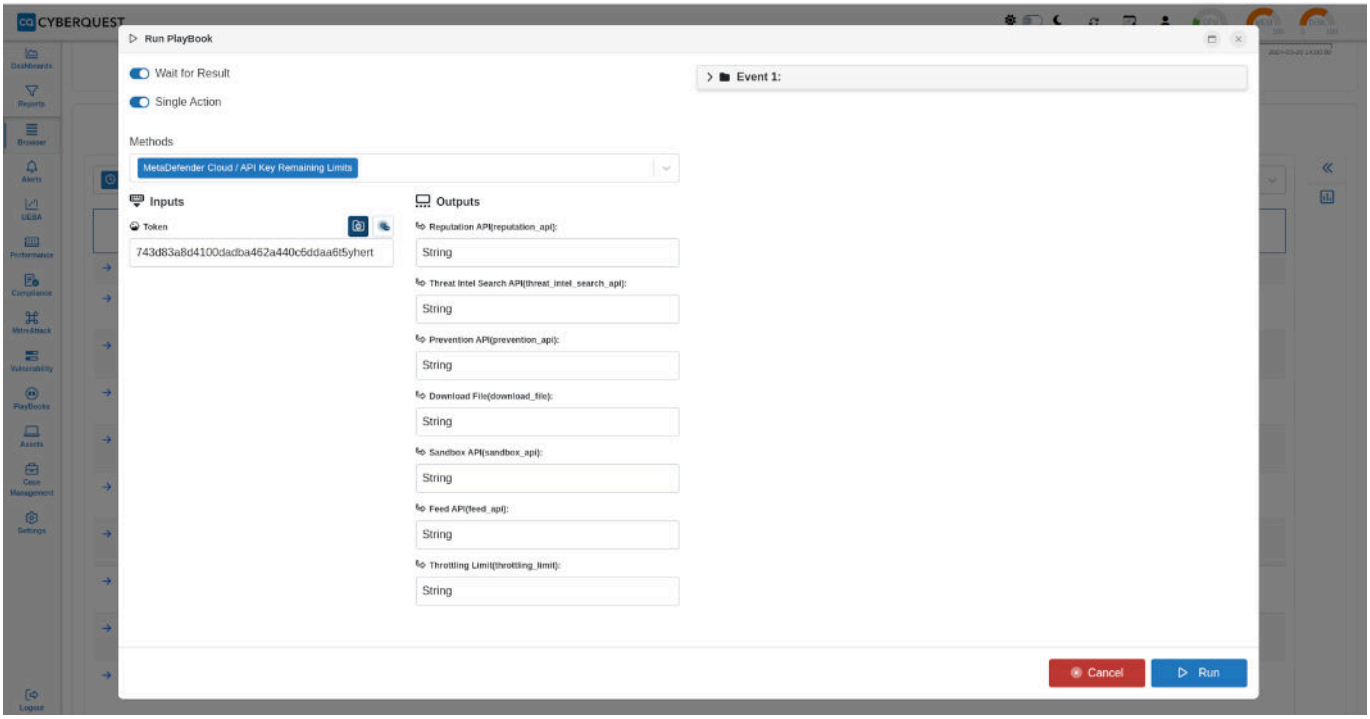


Inputs	Description
Token (is required)	To use the MetaDefenderCloud API, you must have an API key.
limit	How many entries you want to return per request (default is 10000)
offset	How many files you want to skip from the latest request (default is 0)

Outputs	Description
API Key History (data)	The History of API Key

MetaDefender Cloud/API Key Remaining Limits method

Retrieve information about the remaining limits for an apikey.

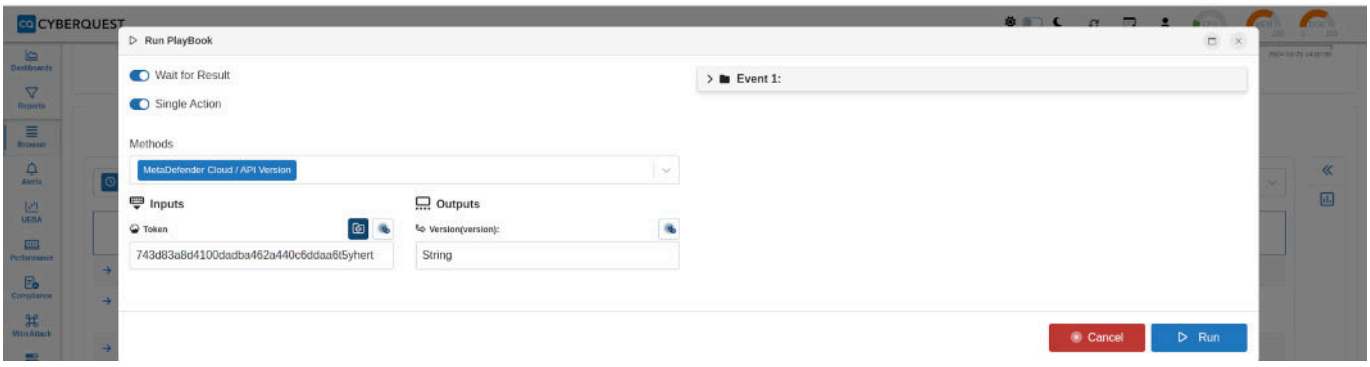


Inputs	Description
Token (is required)	To use the MetaDefenderCloud API, you must have an API key.

Outputs	Description
Reputation API (reputation_api)	The remaining Reputation API limits for the apikey
Threat Intel Search API (threat_intel_search_api)	The remaining Threat Intel Search API limits for the apikey
Prevention API (prevention_api)	The remaining Prevention API limits for the apikey
Download File (download_file)	The remaining limits for file downloads for the apikey
Sandbox API (sandbox_api)	The remaining Dynamic Analysis API limits for the apikey
Feed API (feed_api)	The remaining Feed API limits for the apikey
Throttling Limit (throttling_limit)	The remaining Throttling limits for the apikey

MetaDefender Cloud/API Version method

This endpoint shows the current version of the API.

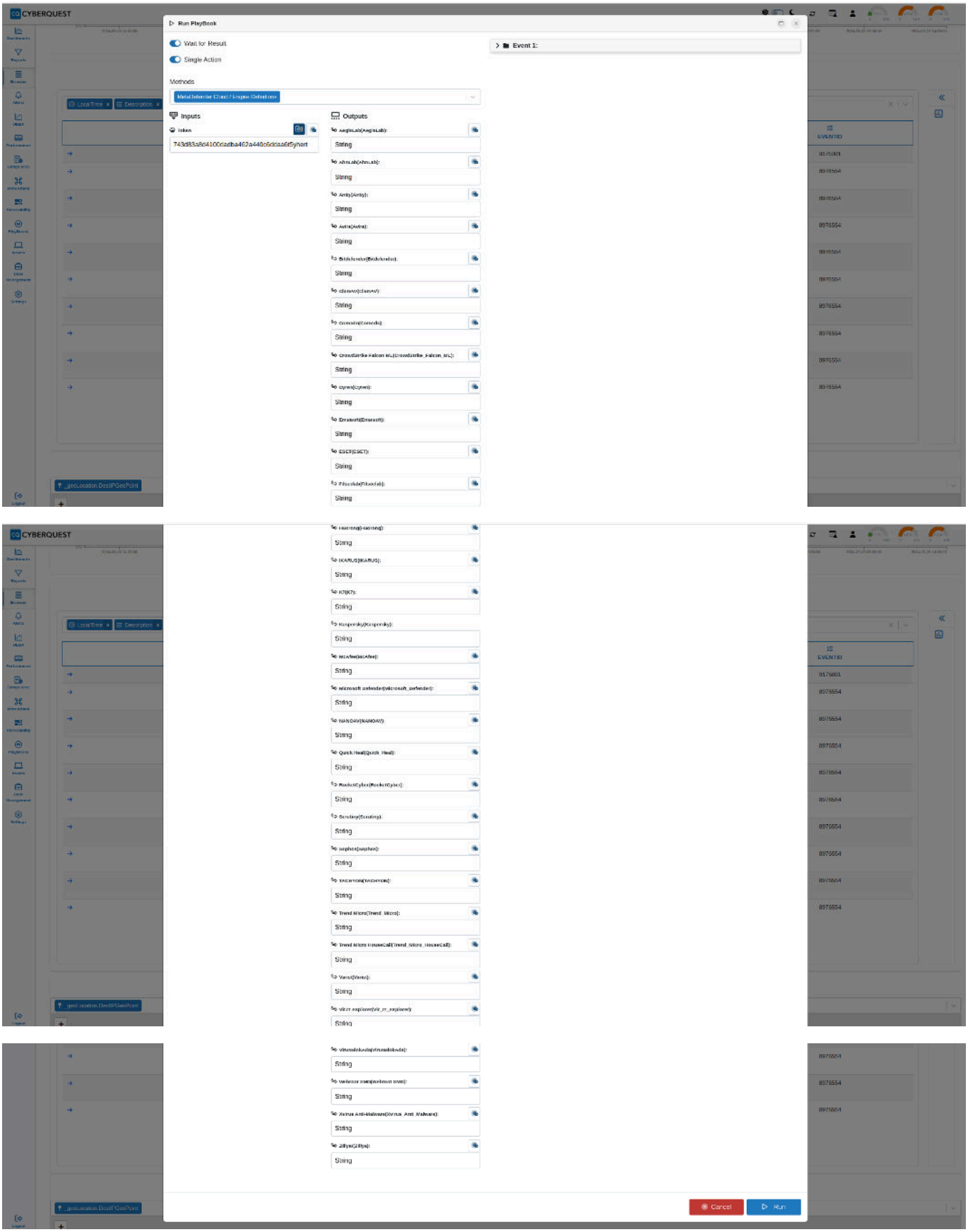


Inputs	Description
Token (is required)	To use the MetaDefenderCloud API, you must have an API key.

Outputs	Description
Version (version)	The version of the current API

MetaDefender Cloud/Engine Definitions method

Returns a list of active anti-malware engines available, as well as the day and time of the engine definition.

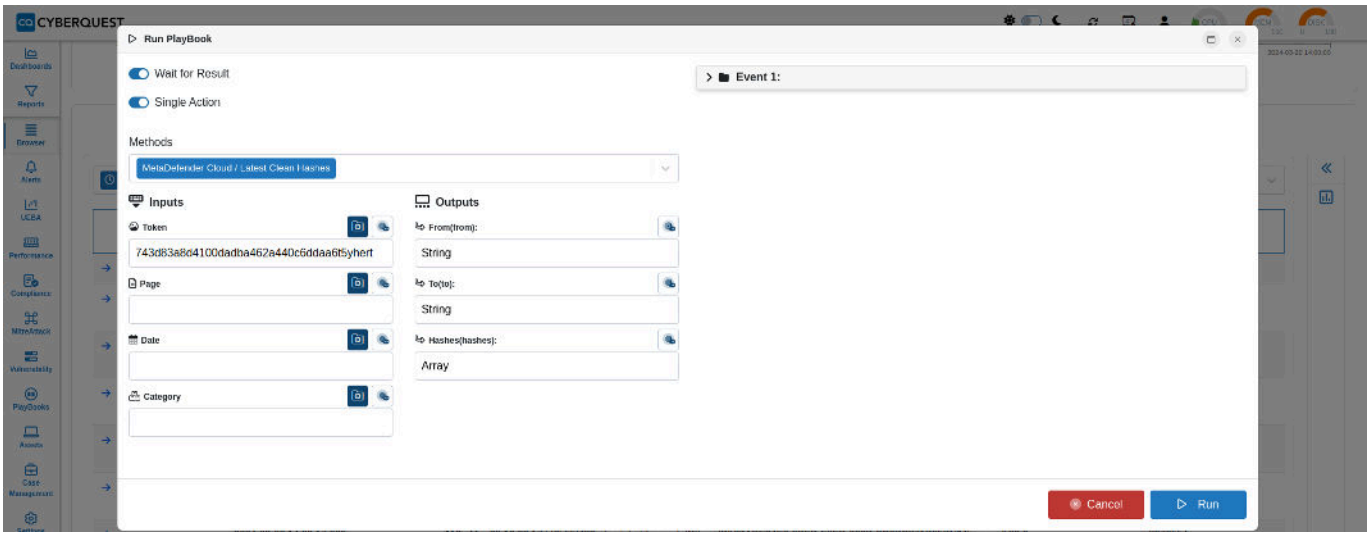


Inputs	Description
Token (is required)	To use the MetaDefenderCloud API, you must have an API key.

Outputs	Description
AegisLab (AegisLab)	Engine used for analysis
AhnLab (AhnLab)	Engine used for analysis
Antiy (Antiy)	Engine used for analysis
Avira (Avira)	Engine used for analysis
Bitdefender (Bitdefender)	Engine used for analysis
ClamAV (ClamAV)	Engine used for analysis
Comodo (Comodo)	Engine used for analysis
CrowdStrike Falcon ML (CrowdStrike_Falcon_ML)	Engine used for analysis
Cyren (Cyren)	Engine used for analysis
Emsisoft (Emsisoft)	Engine used for analysis
ESET (ESET)	Engine used for analysis
Filseclab (Filseclab)	Engine used for analysis
Huorong (Huorong)	Engine used for analysis
IKARUS (IKARUS)	Engine used for analysis
K7 (K7)	Engine used for analysis
Kaspersky (Kaspersky)	Engine used for analysis
McAfee (McAfee)	Engine used for analysis
Microsoft Defender (Microsoft_Defender)	Engine used for analysis
NANOAV (NANOAV)	Engine used for analysis
Quick Heal (Quick_Heal)	Engine used for analysis
RocketCyber (RocketCyber)	Engine used for analysis
Scrutiny (Scrutiny)	Engine used for analysis
Sophos (Sophos)	Engine used for analysis
TACHYON (TACHYON)	Engine used for analysis
Trend Micro (Trend_Micro)	Engine used for analysis
Trend Micro HouseCall (Trend_Micro_HouseCall)	Engine used for analysis
Varist (Varist)	Engine used for analysis
Vir.IT eXplorer (Vir_IT_eXplorer)	Engine used for analysis
Vir.IT ML (Vir_IT_ML)	Engine used for analysis
VirusBlokAda (VirusBlokAda)	Engine used for analysis
Webroot SMD (Webroot SMD)	Engine used for analysis
Xvirus Anti-Malware (Xvirus_Anti_Malware)	Engine used for analysis
Zillya! (Zillya)	Engine used for analysis

MetaDefender Cloud/Latest Clean Hashes method

Sorted chronologically, this feed exposes the latests clean hashes up to 30 days old and is updated continuously. This feed is designed to be used as a live allowlist of hashes to be quarantined.

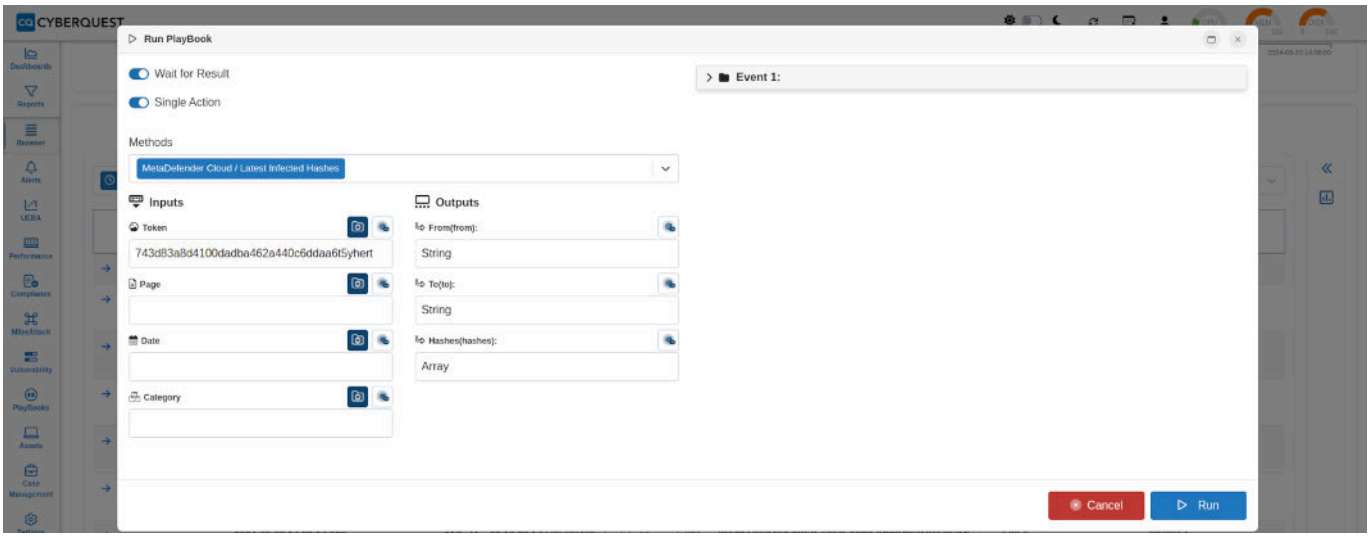


Inputs	Description
Token (is required)	To use the MetaDefenderCloud API, you must have an API key.
Page	This denotes the page number that the data is on (each page has 1000 entries)
Date	Date when the hash was last scanned
Category	File type category. When used, only return hashes of this file type

Outputs	Description
From (from)	Timestamp of the starting point of the data retrieved from the API call.
To (to)	Timestamp of the finishing point of the data retrieved from the API call.
Hashes (hashes)	The list of hashes of the cleaned files

MetaDefender Cloud/Latest Infected Hashes method

This feed exposes the latest infected hashes up to 30 days old and is updated continuously. This feed is designed to be used as a live blocklist of hashes to be quarantined.

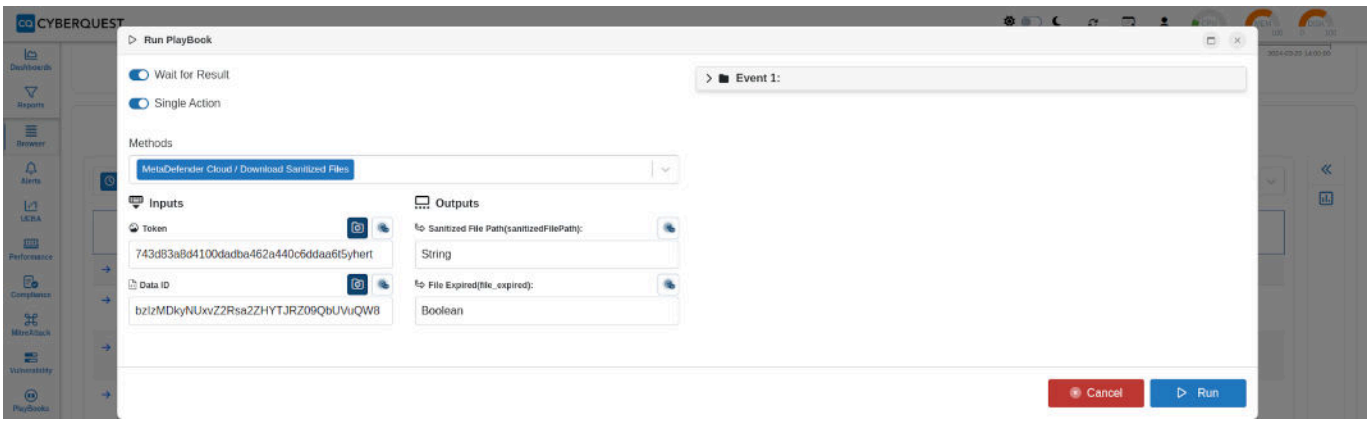


Inputs	Description
Token (is required)	To use the MetaDefenderCloud API, you must have an API key.
Page	This denotes the page number that the data is on (each page has 1000 entries)
Date	Date when the hash was last scanned
Category	File type category. When used, only return hashes of this file type

Outputs	Description
From (from)	Timestamp of the starting point of the data retrieved from the API call.
To (to)	Timestamp of the finishing point of the data retrieved from the API call.
Hashes (hashes)	The list of hashes of the infected files

MetaDefender Cloud/Download Sanitized Files method

Download Sanitized File. The sanitized version of the file is deleted after 24 hours.

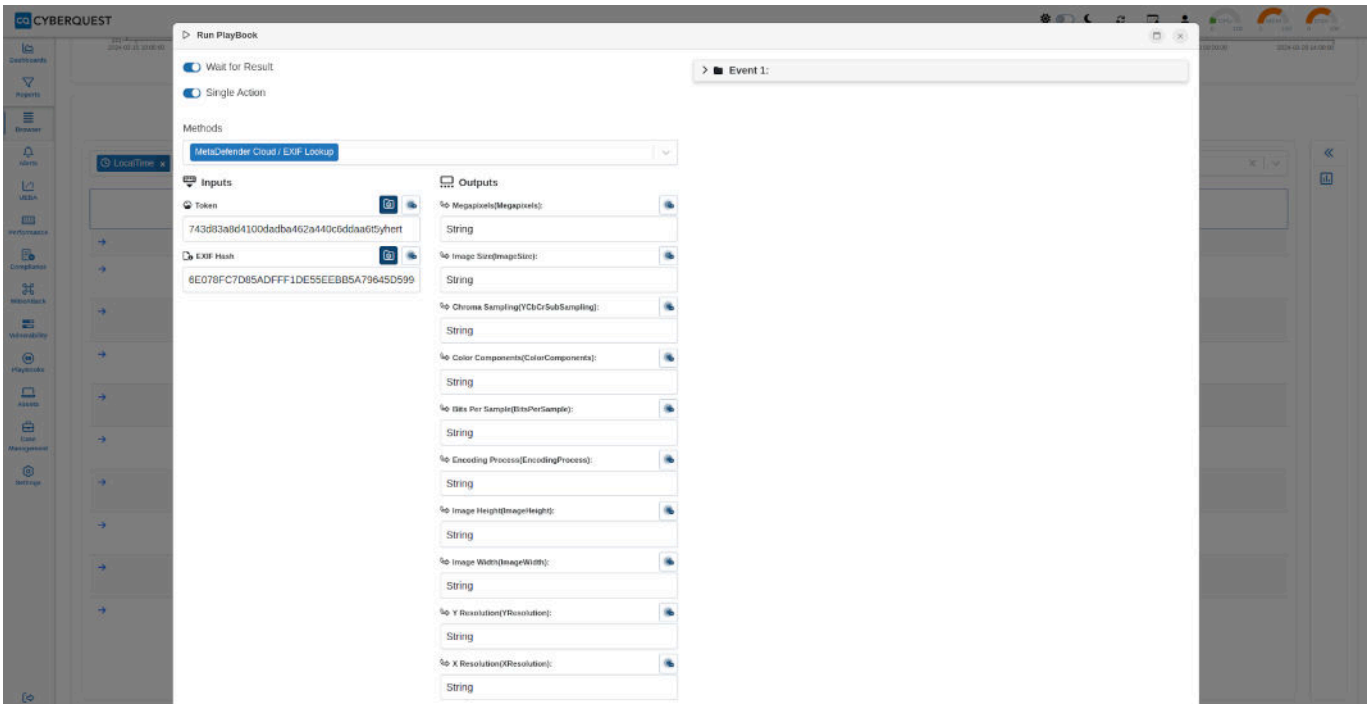


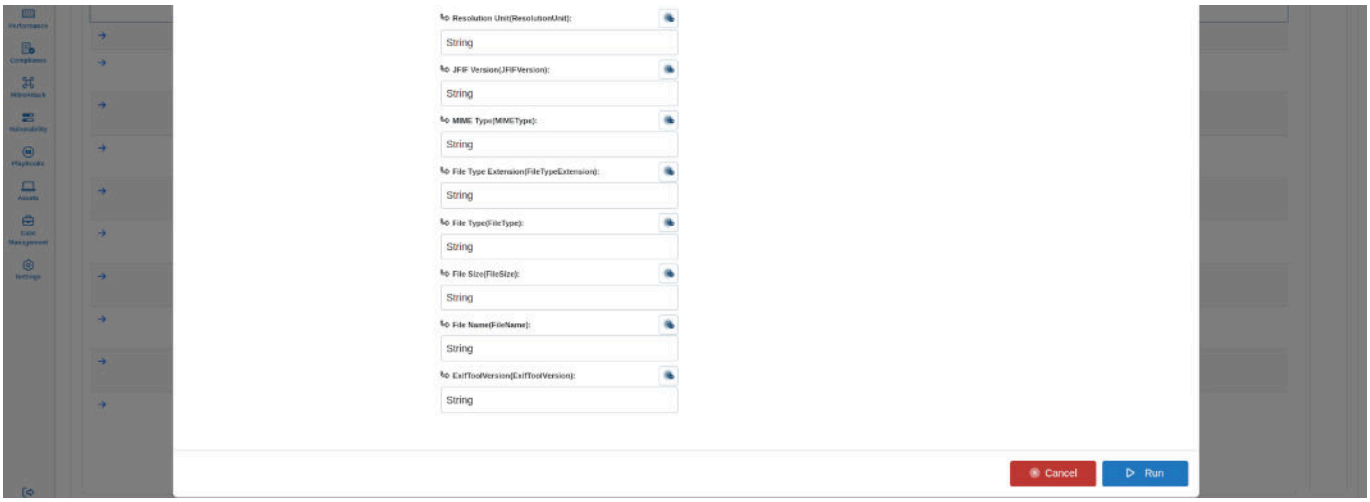
Inputs	Description
Token (is required)	To use the MetaDefenderCloud API, you must have an API key.
Data ID (is required)	The dataId assigned to the file that underwent data sanitization

Outputs	Description
Sanitized File Path (sanitizedFilePath)	The sanitized file
File Expired (file_expired)	The sanitized file

MetaDefender Cloud/EXIF Lookup method

Look up the EXIF of a hash by md5, sha1 or sha256. EXIF is an open standard for storing metadata in images, information like date and time when the image was taken, geolocation of device hardware ID.



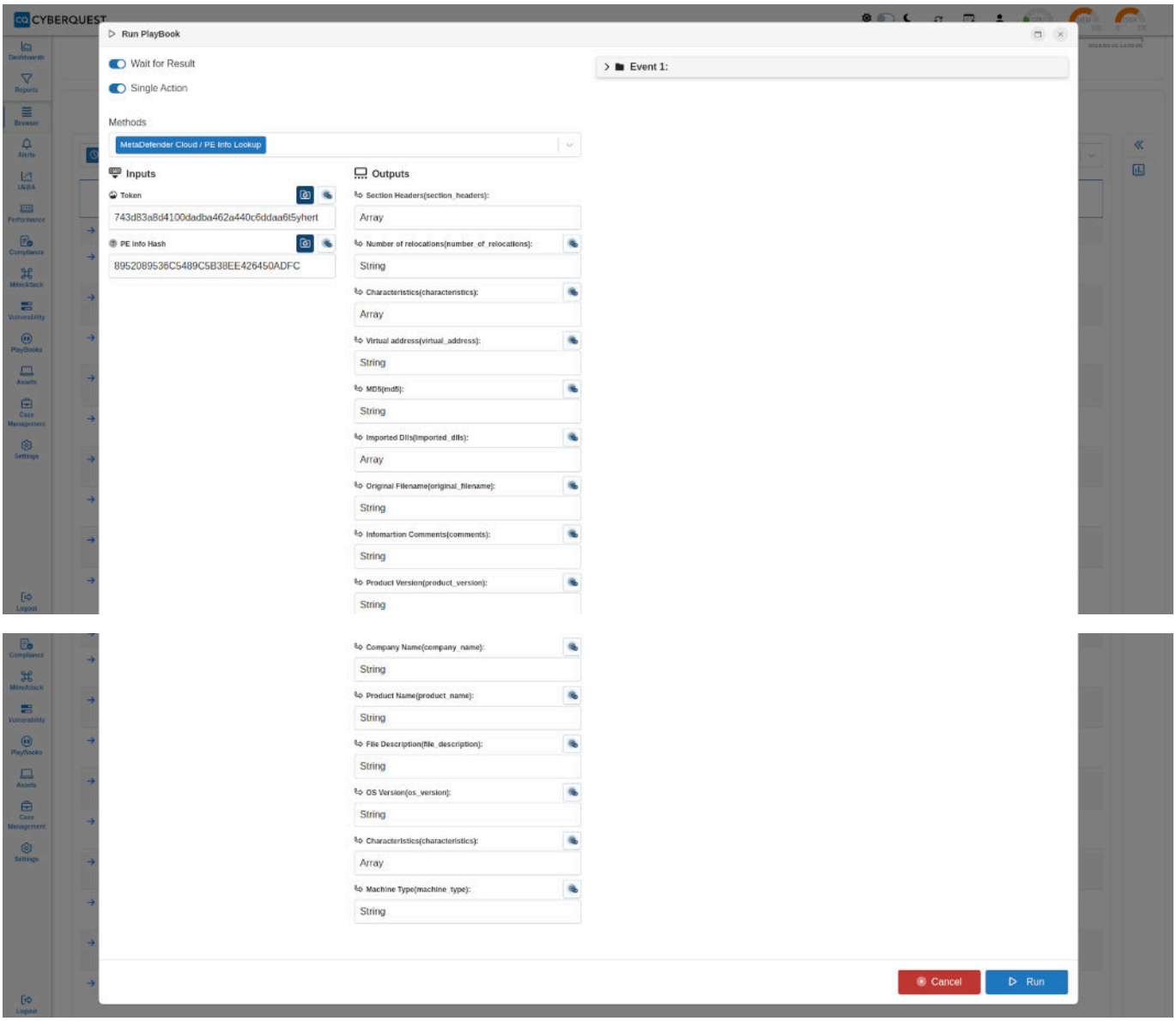


Inputs	Description
Token (is required)	To use the MetaDefenderCloud API, you must have an API key.
EXIF Hash (is required)	The MD5, SHA1 or SHA256 hash that you need exif info for

Outputs	Description
Megapixels (Megapixels)	Provides the resolution information of an image by calculating the total number of pixels in the image.
Image Size (ImageSize)	This parameter provides quick insight into the physical size of the image
Chroma Sampling (YCbCrSubSampling)	This output parameter that indicates the chroma subsampling scheme used in an images color representation. It determines how color information is sampled and compressed, influencing the images quality and file size.
Color Components (ColorComponents)	Provides information about the number and type of color components present in image files metadata. This parameter helps understand the color composition of images and can assist in identifying any anomalies or inconsistencies in color representation within the analyzed images.
Bits Per Sample (BitsPerSample)	This output parameter refers to the information about the number of bits used to represent color or grayscale values in an images pixel data. This parameter helps determine the color depth and quality of the image, aiding in image analysis and understanding its visual characteristics
Encoding Process (EncodingProcess)	It provides insights into the techniques and algorithms employed during the images creation or modification. This parameter can offer valuable metadata for understanding the images origin and processing history.
Image Height (ImageHeight)	Refers to the vertical dimension or height, in pixels, of an image files resolution. This parameter provides essential information about the images size and aspect ratio, aiding in understanding and processing visual content effectively.
Image Width (ImageWidth)	This output parameter that provides the width dimension of an image file in pixels. This parameter offers quick access to the images horizontal size, aiding in understanding its visual characteristics and assisting in further analysis or processing.
Y Resolution (YResolution)	This output parameter represents the vertical resolution of an image. It indicates the number of pixels per unit of measurement (usually inches or centimeters) along the vertical axis. This parameter helps to determine the images clarity and quality in terms of its vertical detail.
X Resolution (XResolution)	This output parameter refers to the horizontal resolution information stored in the Exchangeable Image File Format (EXIF) metadata of an image. This parameter provides details about the number of pixels per unit along the horizontal axis, offering insights into the images quality and dimensions.
Resolution Unit (ResolutionUnit)	This output parameter that indicates the unit of measurement used for image resolution information stored in the Exchangeable Image File Format (EXIF) metadata of an image. This parameter helps determine how the resolution values (width and height) of the image should be interpreted and displayed, whether in pixels per inch (PPI) or pixels per centimeter (PPCM).
JFIF Version (JFIFVersion)	Refers to the version information associated with the JPEG File Interchange Format (JFIF) used in an image files metadata. This parameter indicates the specific version of the JFIF standard that the image follows, providing insights into the images format and compatibility.
MIME Type (MIMEType)	The MIME type provides information about the nature and format of the file, helping to determine how it should be handled or interpreted. This parameter assists in identifying the files content type and guiding appropriate processing or security measures based on the detected MIME type.
File Type Extension (FileTypeExtension)	This output parameter refers to the specific file extension associated with the analyzed image or file
File Type (FileType)	This output parameter provides information about the specific type or format of the image file being analyzed.
File Size (FileSize)	Provides information about the size of the file being analyzed
File Name (FileName)	This output parameter represents the name of the file being analyzed.
ExifToolVersion (ExifToolVersion)	Version information of the ExifTool software used to extract and process metadata from files

MetaDefender Cloud/PE Info Lookup method

Look up the PE (portable executable file format) info of a hash by MD5, SHA1 or SHA256. With PE info specifications for executable files information like executable headers, section headers, import and export tables, application resources and others can be viewed and analyzed.

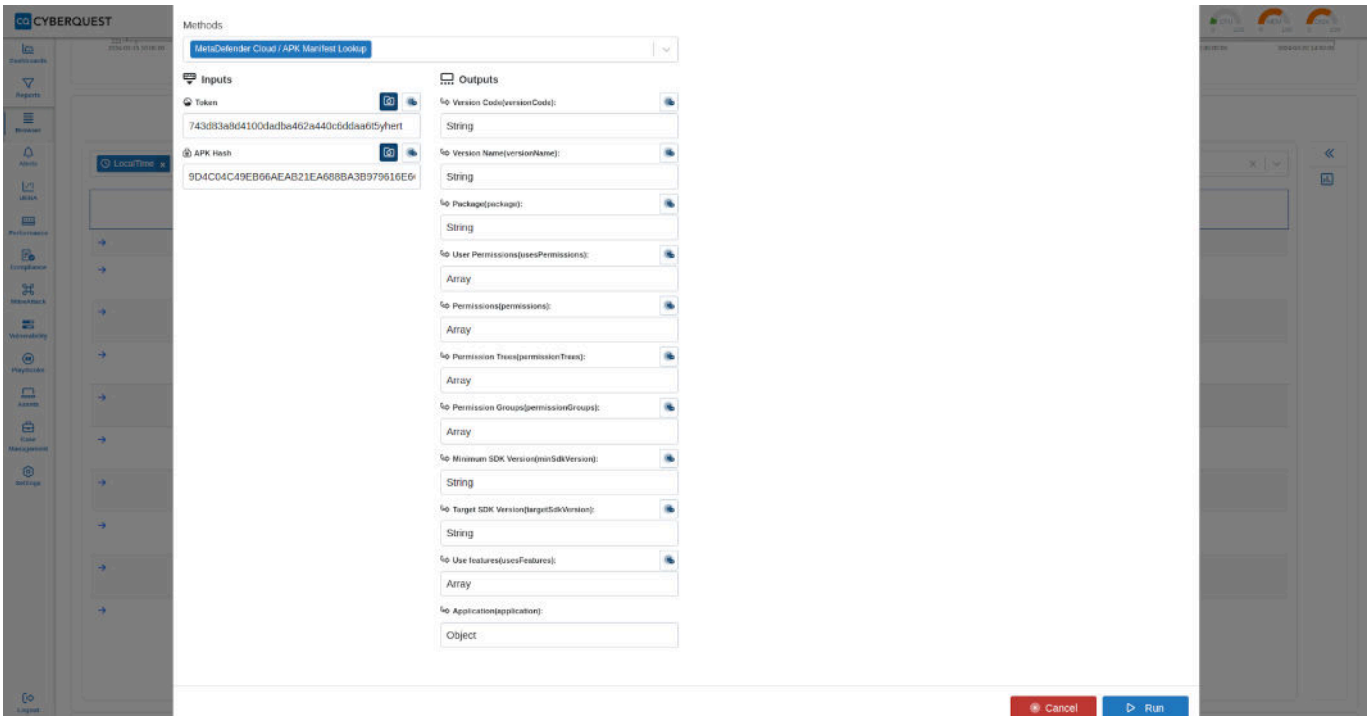


Inputs	Description
Token (is required)	To use the MetaDefenderCloud API, you must have an API key.
PE Info Hash (is required)	The MD5, SHA1 or SHA256 hash that you need PE info for

Outputs	Description
Section Headers (section_headers)	Metadata and characteristics of the sections within the PE file
Number of relocations (number_of_relocations)	This parameter helps analyze potential code modifications or tampering in the file, aiding in identifying suspicious or altered software components
Characteristics (characteristics)	Provides key attributes and properties of a Portable Executable (PE) file. These characteristics include information about the files structure, behavior, and capabilities, aiding in the analysis and understanding of the files potential impact on a system
Virtual address (virtual_address)	This output parameter represents the memory address where a specific element within a Portable Executable (PE) file is loaded when the file is executed. This parameter provides crucial information about the files internal structure and layout, aiding in understanding how the file functions within a computers memory during runtime
MD5 (md5)	Provide the MD5 hash of the PE file being analyzed
Imported Dlls (imported_dlls)	Refers to a list of Dynamic Link Libraries (DLLs) that a Portable Executable (PE) file, often an executable or a binary, depends on. These DLLs are external components that the PE file needs to execute properly
Original Filename (original_filename)	This information offers insights into the initial name of the file before any potential renaming or modification occurred
Infomartion Comments (comments)	Parameter provides supplementary textual notes or comments associated with the version information of a PE file, offering insights into the purpose, updates, or other relevant details about the executable
Product Version (product_version)	This data reveals the version of the software or application that created the file, aiding in software identification and compatibility assessment
Company Name (company_name)	This parameter provides insight into the company or organization associated with the creation or distribution of the analyzed file, aiding in identifying its source and potential legitimacy.
Product Name (product_name)	The name of the product from the version information embedded within a PE file
File Description (file_description)	Description of file
OS Version (os_version)	This parameter offers insights into the specific version of the operating system for which the PE file was designed, aiding in compatibility and security assessments
Characteristics (characteristics)	This parameter offers valuable insights into the structural and operational aspects of the PE file
Machine Type (machine_type)	This helps identify the target architecture for which the file is intended, aiding in compatibility and analysis

MetaDefender Cloud/APK Manifest Lookup method

Look up the APK manifest analysis of a hash by MD5, SHA1 or SHA256.

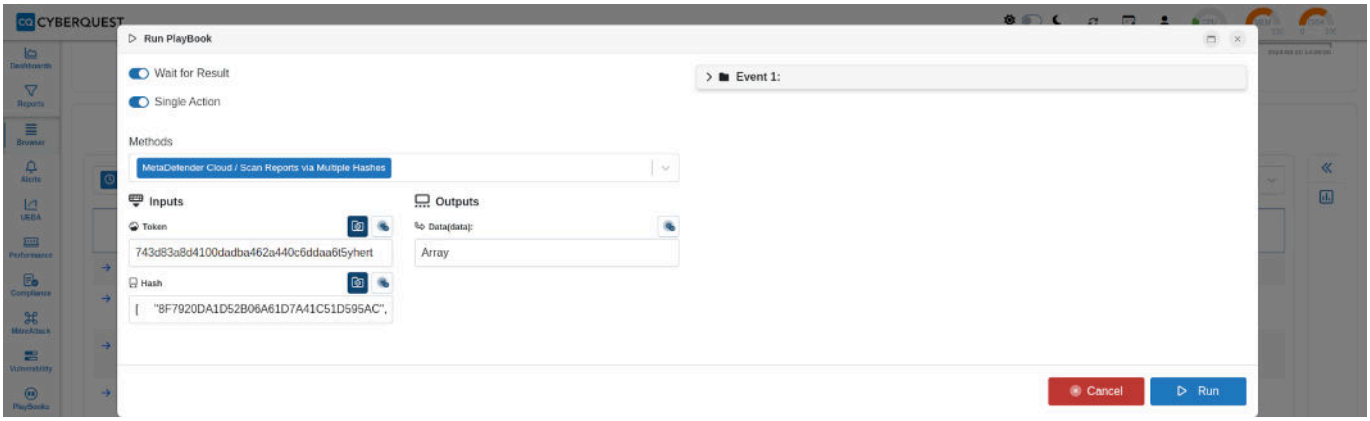


Inputs	Description
Token (is required)	To use the MetaDefenderCloud API, you must have an API key.
APK Hash (is required)	The MD5, SHA1 or SHA256 hash containing the Android Manifest information

Outputs	Description
Version Code (versionCode)	This value helps uniquely identify and track different versions of the app, assisting in app management, updates, and compatibility checks.
Version Name (versionName)	Refers to a field that specifies the human-readable version of an Android application. It helps users identify and understand the version of the app being analyzed.
Package (package)	Refers to the unique identifier assigned to an Android application. This identifier is crucial for distinguishing and managing different apps, aiding in their proper installation, updates, and security assessment.
User Permissions (usesPermissions)	A list of permissions requested by an Android app (APK). These permissions indicate what actions or resources the app can access on a users device, helping to assess potential security and privacy risks associated with the apps behavior.
Permissions (permissions)	A list of permissions requested by an Android apps APK file. These permissions indicate the actions and resources the app can access on a users device, helping to assess potential security and privacy implications.
Permission Trees (permissionTrees)	Refers to a specific output parameter that provides information about hierarchical permission relationships within an Android application (APK). It outlines the permissions requested by the app and their interconnections, helping to understand how different permissions relate to one another in the apps structure.
Permission Groups (permissionGroups)	The Sets of permissions within Android apps that share related functionalities.
Minimum SDK Version (minSdkVersion)	Indicates the minimum Android operating system version required for the analyzed Android app (APK file) to function correctly.
Target SDK Version (targetSdkVersion)	This parameter refers to the designated version of the Android software development kit (SDK) that the Android app is specifically designed to target.
Use features (usesFeatures)	This parameter indicates the hardware and software features that an Android application (APK) utilizes or requires to function properly on a device.
Application (application)	

MetaDefender Cloud/Scan Reports via Multiple Hashes method

Look up the scan results based on MD5, SHA1, or SHA256 for multiple data hashes.

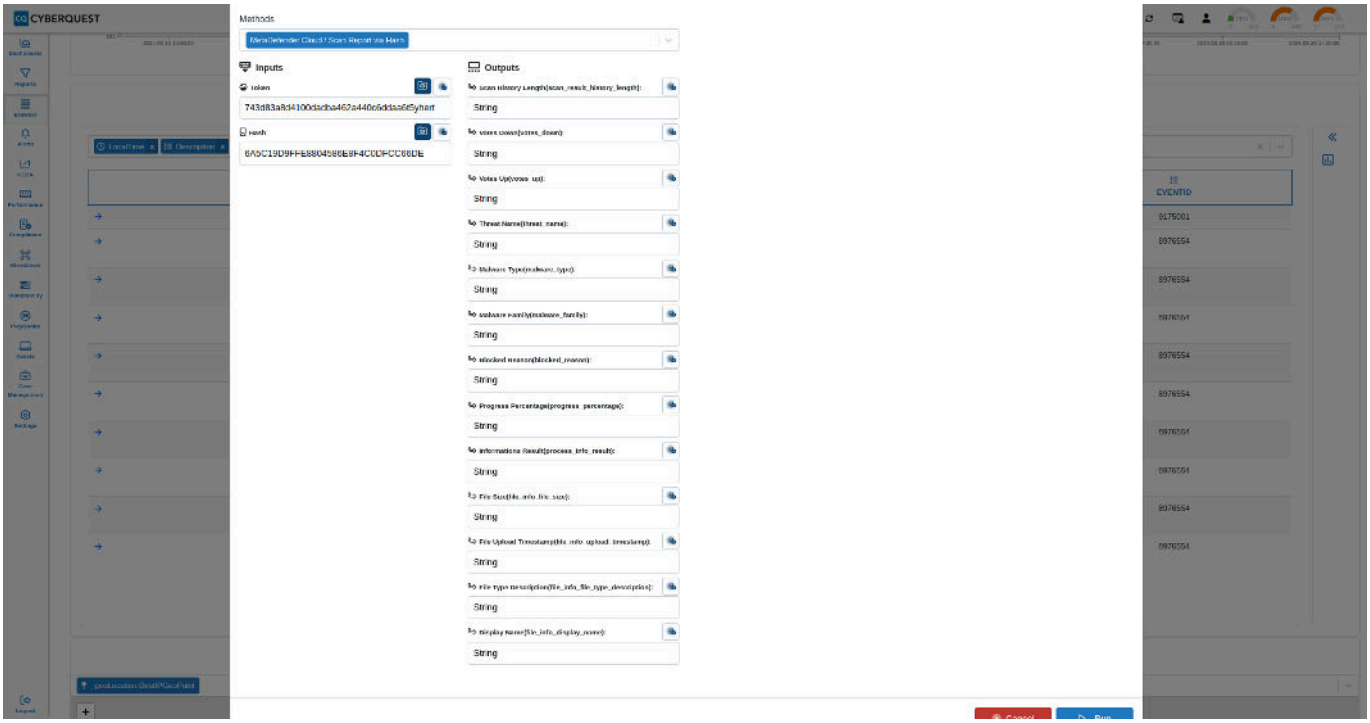


Inputs	Description
Token (is required)	To use the MetaDefenderCloud API, you must have an API key.
Hash (is required)	A list of hashes what is used to identify files (MD5, SHA1 or SHA256)

Outputs	Description
Data (data)	The results of the reports

MetaDefender Cloud/Scan Report via Hash method

Retrieve scan reports by looking up a hash using MD5, SHA1 or SHA256.

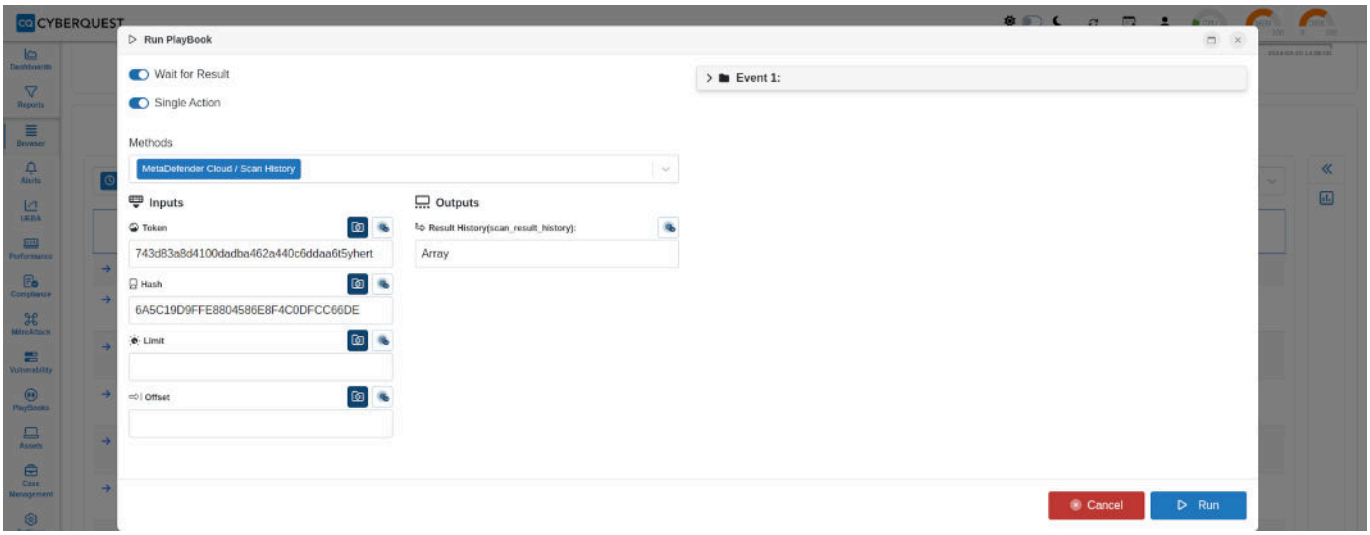


Inputs	Description
Token (is required)	To use the MetaDefenderCloud API, you must have an API key.
Hash (is required)	The MD5, SHA1 or SHA256 hash you want to look up information for

Outputs	Description
Scan History Length (scan_result_history_length)	How many historical scan results for a particular file or resource are stored and accessible.
Votes Down (votes_down)	The number of the votes from community
Votes Up (votes_up)	The number of the votes from community
Threat Name (threat_name)	The name of the threat detected
Malware Type (malware_type)	Provides essential information gained from analyzing malicious software.
Malware Family (malware_family)	This output parameter categorizes specific types of malicious software based on shared characteristics and behaviors
Blocked Reason (blocked_reason)	The reason of the block
Progress Percentage (progress_percentage)	The progress of the analyses
Informations Result (process_info_result)	The action what was taken after the scan of the file
File Size (file_info_file_size)	The size of file
File Upload Timestamp (file_info_upload_timestamp)	The exact date and time when the file was uploaded to platform
File Type Description (file_info_file_type_description)	Descriptive representation of the format of a file
Display Name (file_info_display_name)	User-friendly label associated with a particular entity

MetaDefender Cloud/Scan History method

Look up the scan history of a hash by MD5, SHA1, or SHA256 (some scan histories can have hundreds of entries).

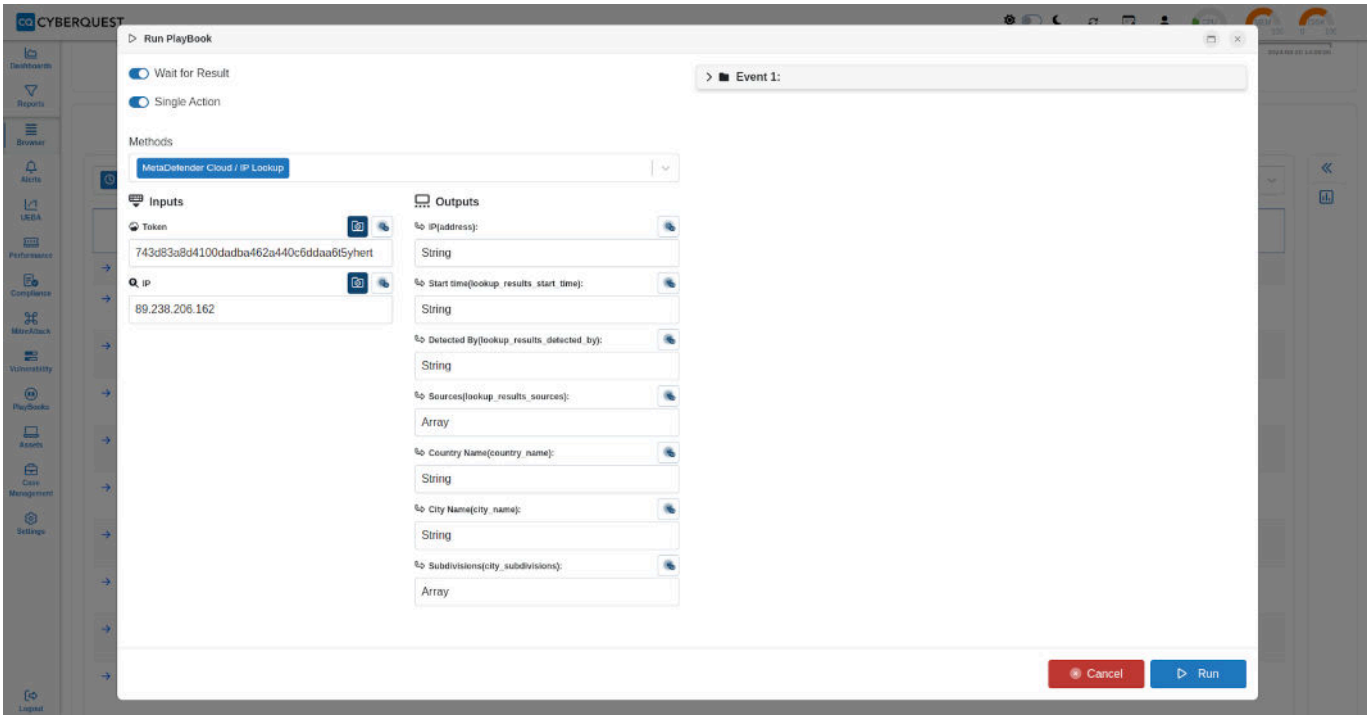


Inputs	Description
Token (is required)	To use the MetaDefenderCloud API, you must have an API key.
Hash (is required)	The MD5, SHA1 or SHA256 hash for the file that you want the scan history for
Limit	Pagination - how many entries you want to return
Offset	Pagination - how many entries to skip (sorted chronologically)

Outputs	Description
Result History (scan_result_history)	Scan history of the hash

MetaDefender Cloud/IP Lookup method

Retrieve information about given IP (IPv4 + IPv6) from a CIF server.

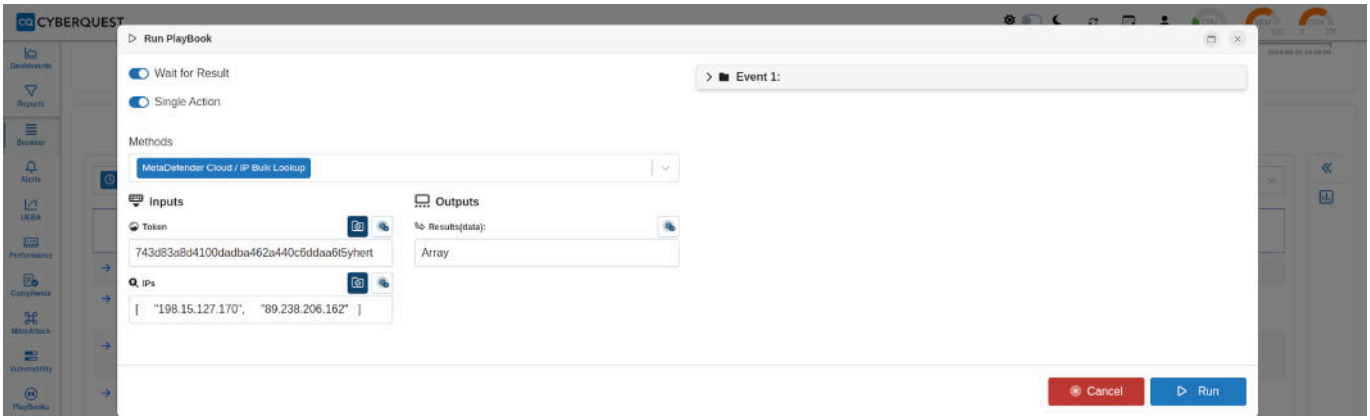


Inputs	Description
Token (is required)	To use the MetaDefenderCloud API, you must have an API key.
IP (is required)	MD5 or SHA256 hash of a submitted file

Outputs	Description
IP (address)	The IP which is investigated
Start time (lookup_results_start_time)	The start time of the investigations
Detected By (lookup_results_detected_by)	The number of antiviruses used in scan
Sources (lookup_results_sources)	The result of antiviruses used in analysis
Country Name (country_name)	The country where the IP originates
City Name (city_name)	The city where the IP originates
Subdivisions (city_subdivisions)	More details about geolocations

MetaDefender Cloud/IP Bulk Lookup method

Retrieve information about a list of IPs (Pv4/IPv6).

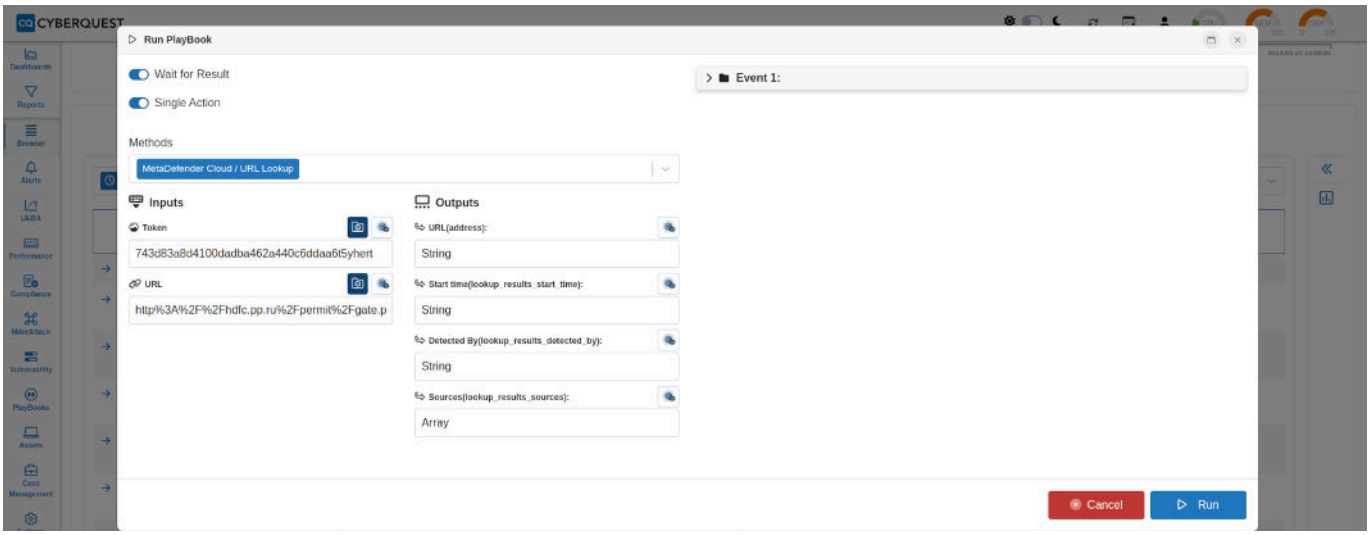


Inputs	Description
Token (is required)	To use the MetaDefenderCloud API, you must have an API key.
IPs (is required)	An array of IPs for investigations

Outputs	Description
Results (data)	The result of the lookup

MetaDefender Cloud/URL Lookup method

Retrieve information about given observable (URL) from a CIF server.

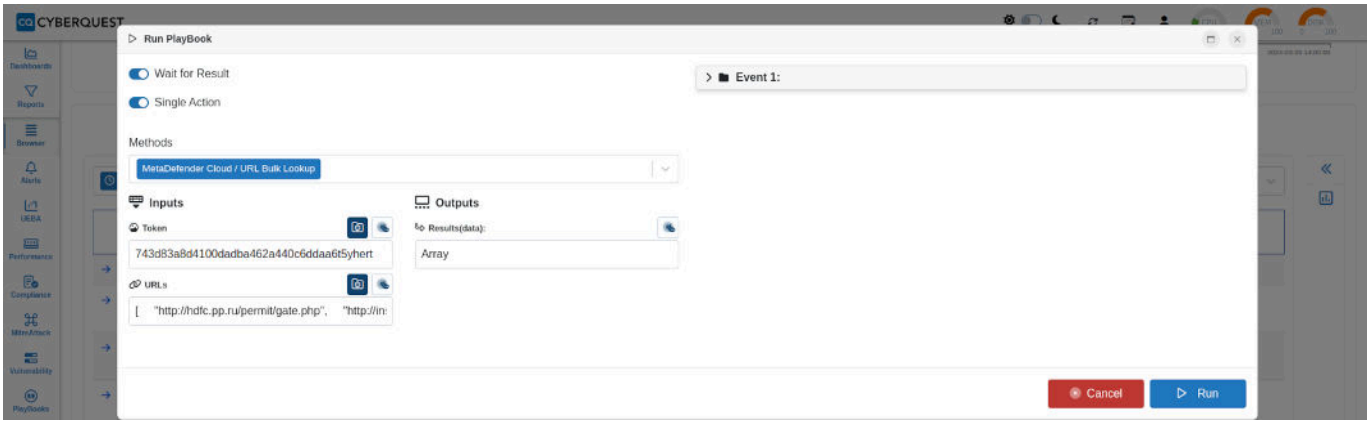


Inputs	Description
Token (is required)	To use the MetaDefenderCloud API, you must have an API key.
URL (is required)	The URL which is investigated

Outputs	Description
URL (address)	The URL investigated
Start time (lookup_results_start_time)	The start time of the investigation
Detected By (lookup_results_detected_by)	The number of antiviruses used in scan
Sources (lookup_results_sources)	The result from antiviruses used in analysis

MetaDefender Cloud/URL Bulk Lookup method

Retrieve information about a list of given observables (URLs) from a CIF server.

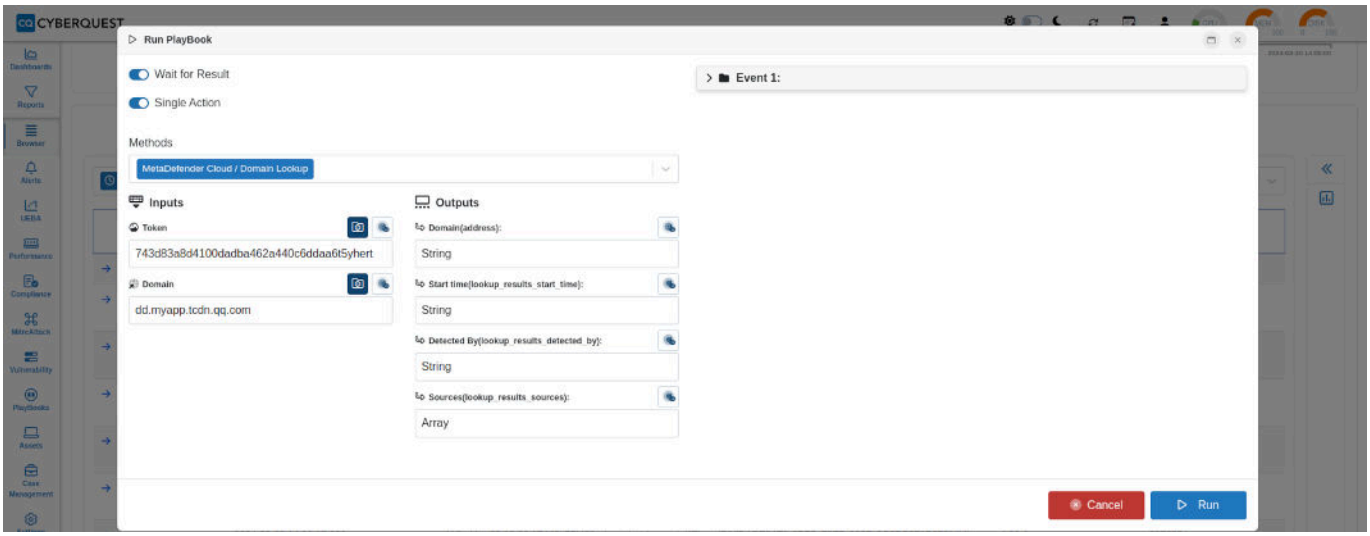


Inputs	Description
Token (is required)	To use the MetaDefenderCloud API, you must have an API key.
URLs (is required)	An array of URLs which will be investigated

Outputs	Description
Results (data)	The results of the lookup

MetaDefender Cloud/Domain Lookup method

Retrieve information about a given fully qualified domain name (FQDN) from a CIF server including but not limited to: provider of the FQDN, a security assessment about the FQDN, and time of detection.

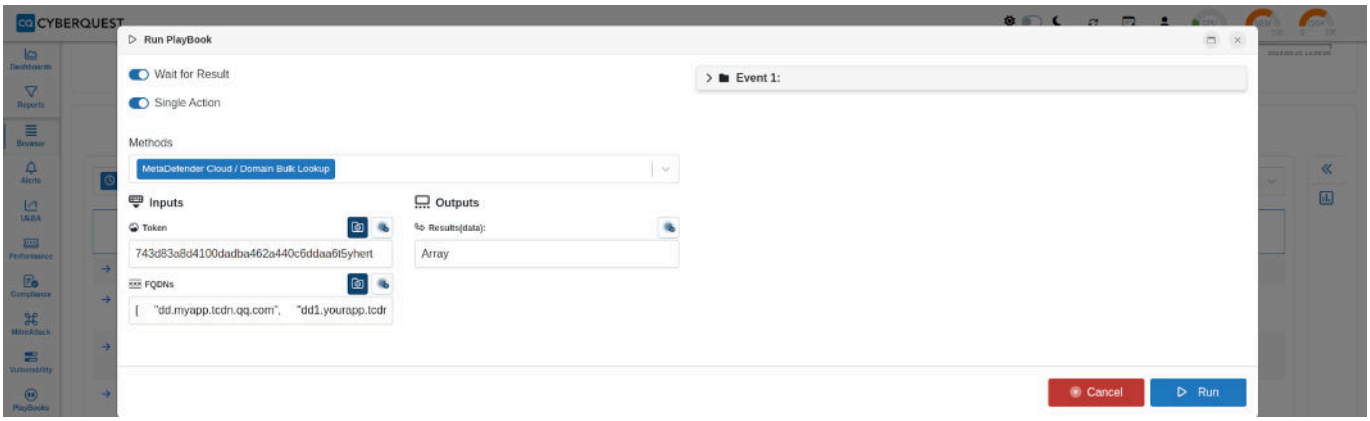


Inputs	Description
Token (is required)	To use the MetaDefenderCloud API, you must have an API key.
Domain (is required)	The investigated domain

Outputs	Description
Domain (address)	The investigated result
Start time (lookup_results_start_time)	The start time of the investigation
Detected By (lookup_results_detected_by)	The number of antiviruses used in scan
Sources (lookup_results_sources)	The result of antiviruses used in analysis

MetaDefender Cloud/Domain Bulk Lookup method

Retrieve information about a list of fully qualified domain names (FQDNs) from a CIF server including but not limited to: provider of the FQDNs, a security assessment about the FQDNs, and time of detection.

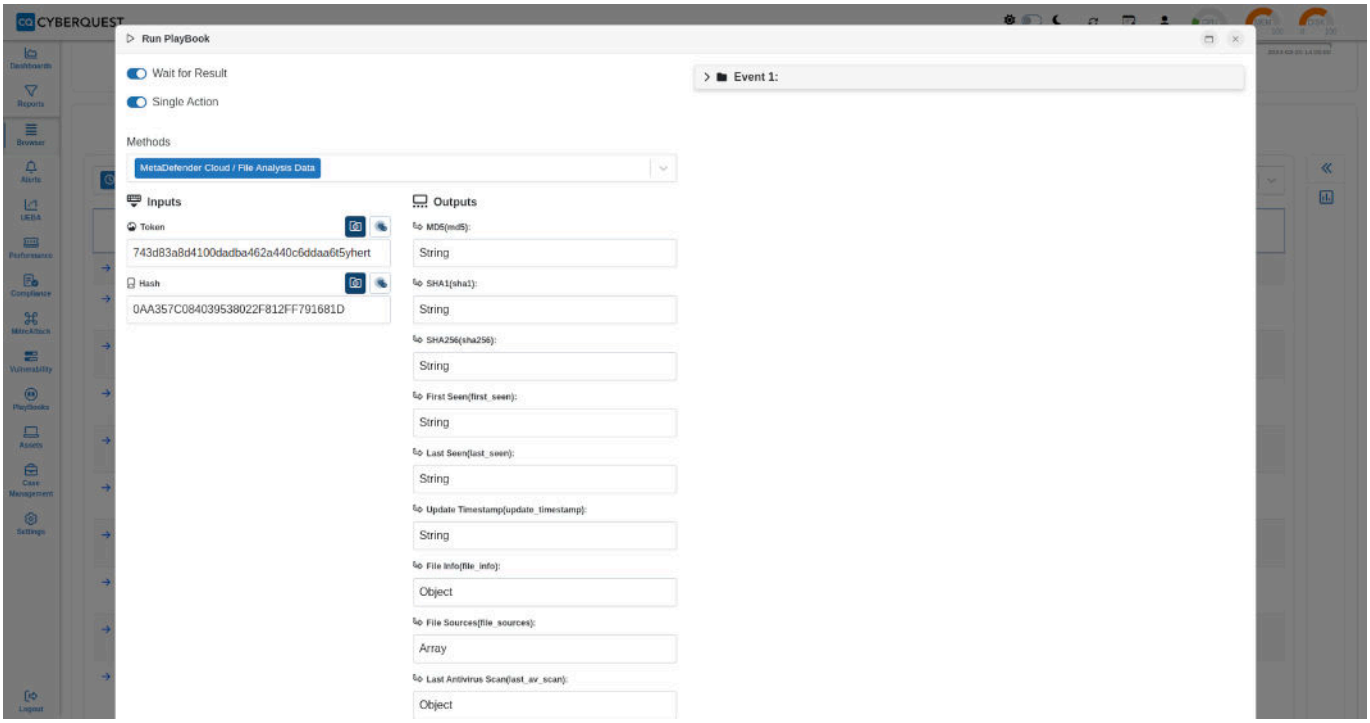


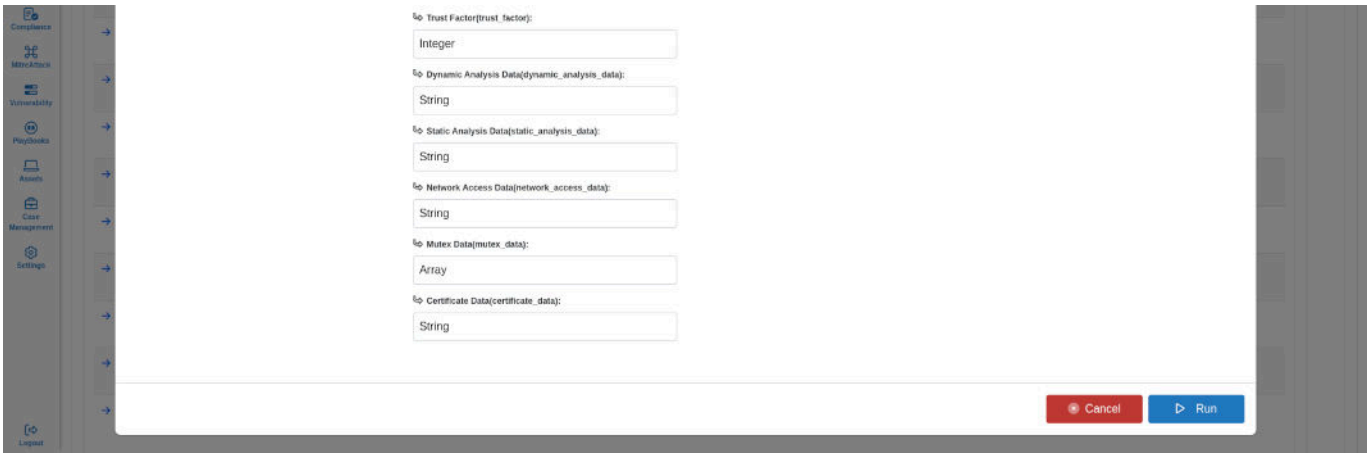
Inputs	Description
Token (is required)	To use the MetaDefenderCloud API, you must have an API key.
FQDNs (is required)	An array with investigated domain

Outputs	Description
Results (data)	The result of the lookup

MetaDefender Cloud/File Analysis Data method

Provides file analysis data on hashes (MD5, SHA1, or SHA256). Metadata can include relevant portions of static and dynamic analysis, AV scan information, file sources.



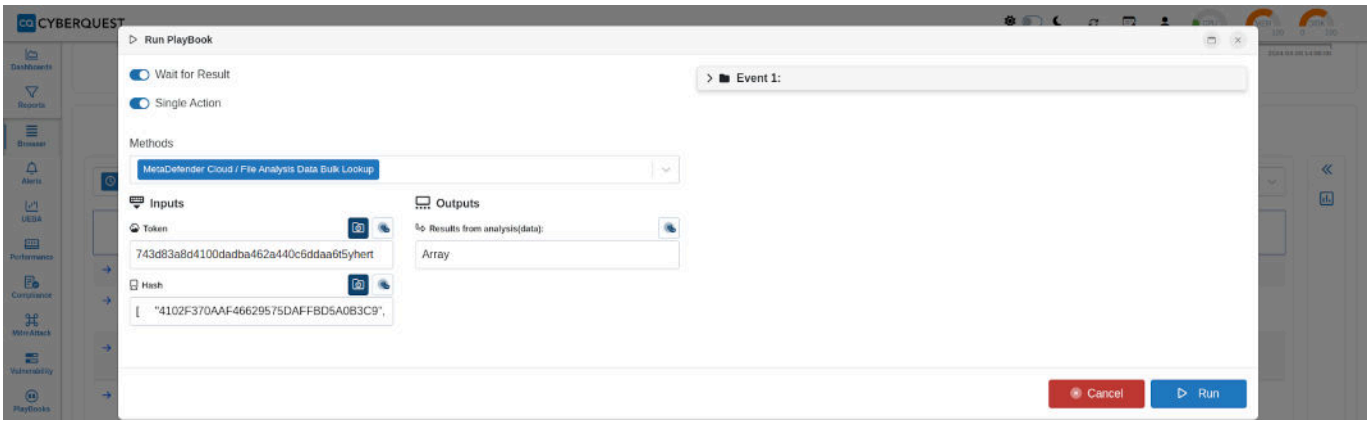


Inputs	Description
Token (is required)	To use the MetaDefenderCloud API, you must have an API key.
Hash (is required)	A hash is used to identify a file (MD5, SHA1 or SHA256)

Outputs	Description
MD5 (md5)	MD5 of analyzed file
SHA1 (sha1)	SHA1 of analyzed file
SHA256 (sha256)	SHA256 of analyzed file
First Seen (first_seen)	The timestamp when the file was first time seen
Last Seen (last_seen)	The timestamp when the file was first last time seen
Update Timestamp (update_timestamp)	The timestamp when the previous timestamp was updated
File Info (file_info)	Information about the file
File Sources (file_sources)	Informations about the file sources
Last Antivirus Scan (last_av_scan)	Informations about last antivirus scan
Trust Factor (trust_factor)	The value of trust calculated by MetaDegfender
Dynamic Analysis Data (dynamic_analysis_data)	The value of Dynamic Analysis Data
Static Analysis Data (static_analysis_data)	The value of Static Analysis Data
Network Access Data (network_access_data)	The value of Network Access Data
Mutex Data (mutex_data)	Informations about mutex
Certificate Data (certificate_data)	The timestamp of certificate

MetaDefender Cloud/File Analysis Data Bulk Lookup method

Bulk lookup of file analysis data on hashes (MD5, SHA1, or SHA256). Metadata can include relevant portions of static and dynamic analysis, AV scan information, file sources.

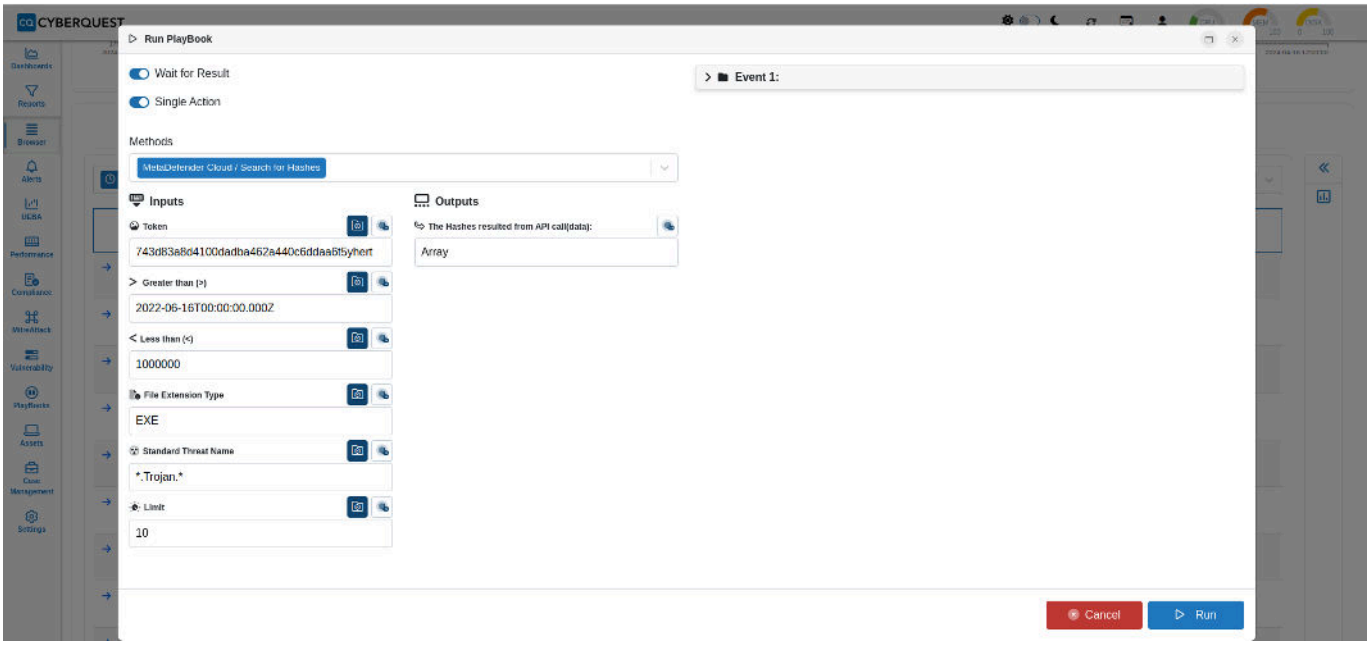


Inputs	Description
Token (is required)	To use the MetaDefenderCloud API, you must have an API key.
Hash (is required)	A hash is used to identify a file (MD5, SHA1 or SHA256)

Outputs	Description
Results from analysis (data)	The results from analysis

MetaDefender Cloud/Search for Hashes method

Search for hashes using multi-part search criteria.



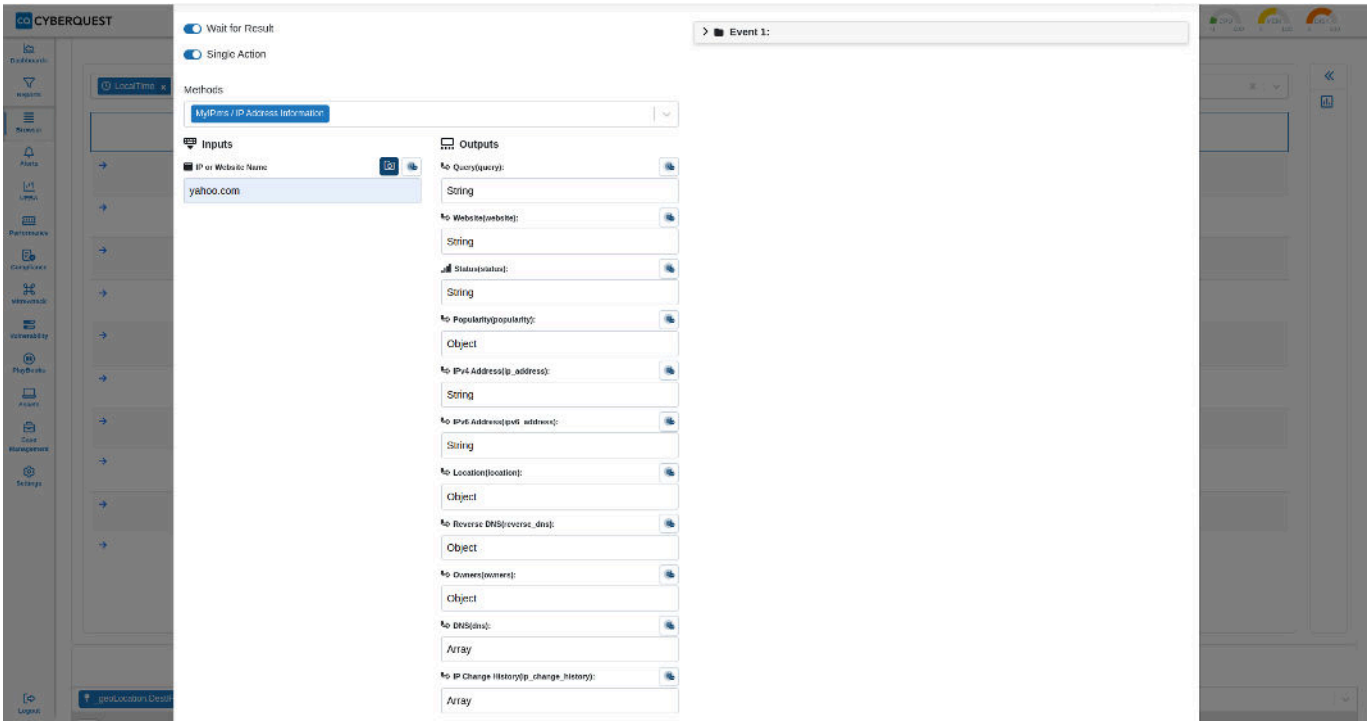
Inputs	Description
Token (is required)	To use the MetaDefenderCloud API, you must have an API key.
Greater than (>) (is required)	Comparison Operator
Less than (<) (is required)	Comparison Operator
File Extension Type (is required)	The extension of the file
Standard Threat Name (is required)	This parameter refers to the recognized and standardized name given to a specific type of threat or malware
Limit (is required)	Maximum Responses Received

Outputs	Description
The Hashes resulted from API call (data)	The result of the request

MyIp.ms

MyIP.ms/IP Address Information method

Get information about IP addresses.



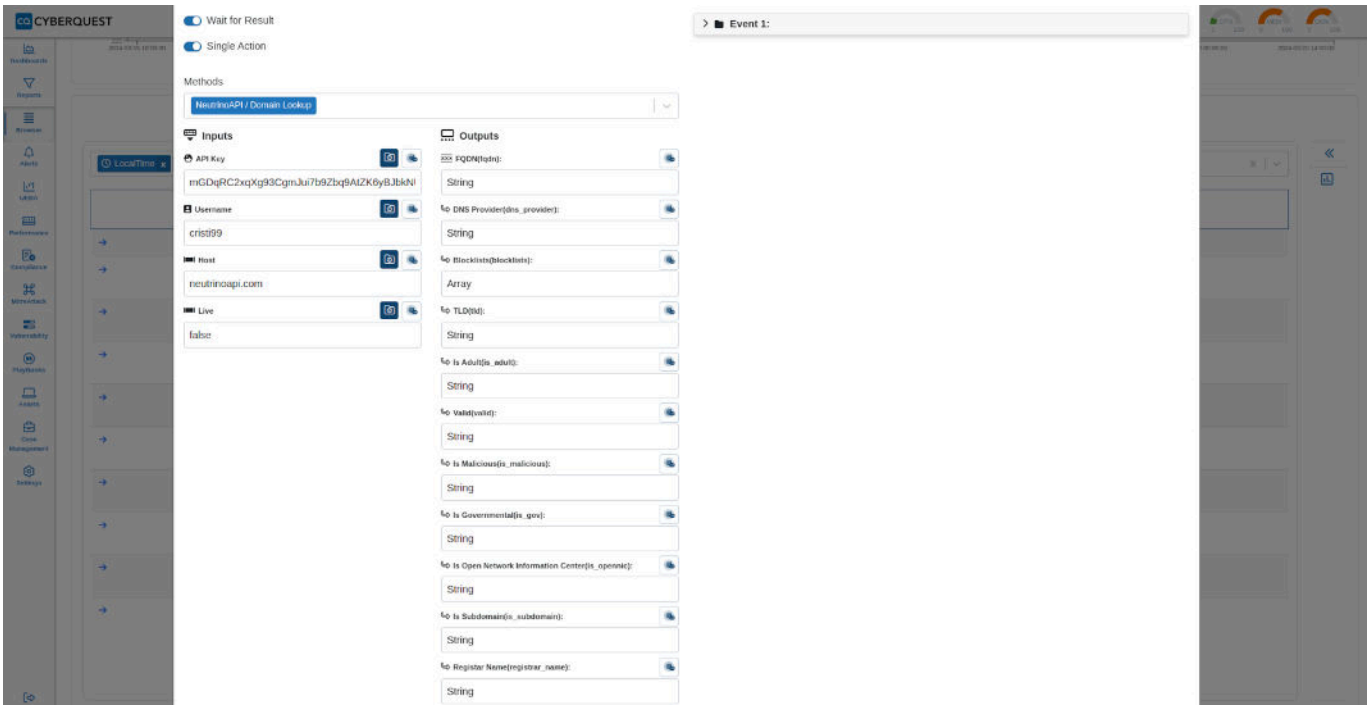
Inputs	Description
IP or Website Name (is required)	The IP or Website Name which is investigated

Outputs	Description
Query (query)	The investigated IP or Domain
Website (website)	Full site name
Status (status)	The status of the API call
Popularity(popularity)	Details about popularity of the investigated IP or Domain
IPv4 Address(ip_address)	IPv4 address
IPv6 Address(ipv6_address)	IPv6 address
Location(location)	The location of the investigated IP or Domain
Reverse DNS(reverse_dns)	Details about Reverse DNS
Owners(owners)	Details about the owners of the IP or Domain investigated
DNS(dns)	A list of multiple DNS servers
IP Change History(ip_change_history)	Details about IP changes

Neutrino API

NeutrinoAPI/Domain Lookup method

Parse, validate and get detailed user-agent information from a user agent string or from client hints.

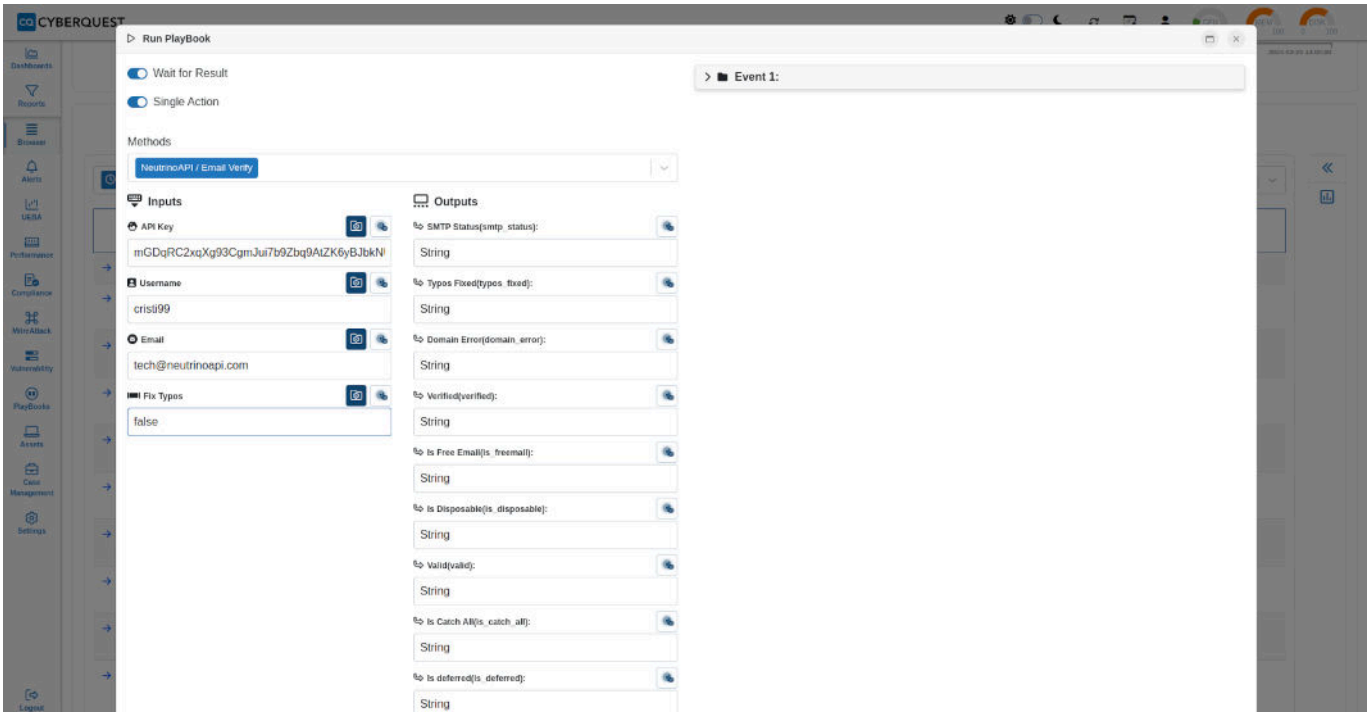


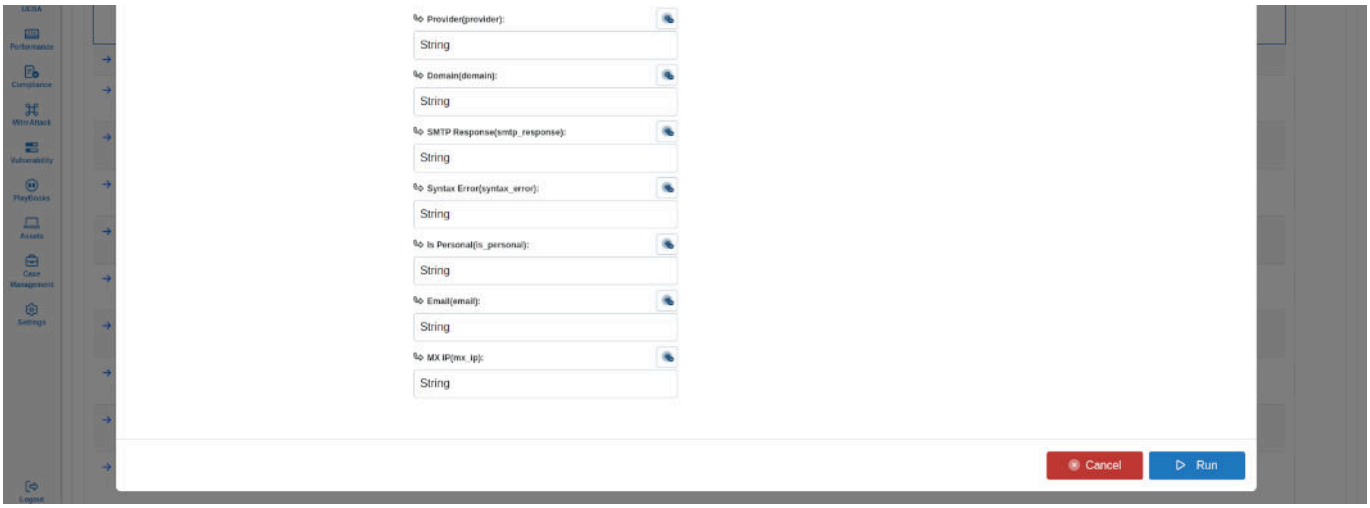
Inputs	Description
API Key (is required)	To use this API you must have an API Key from Neutrino Website
Username (is required)	The username used to Login on Neutrino Website
Host (is required)	A domain name, hostname, FQDN, URL, HTML link or email address to lookup
Live	For domains that we have never seen before then perform various live checks and realtime reconnaissance.NOTE: this option may add additional non-deterministic delay to the request, if you require consistently fast API response times or just want to check our domain blocklists then you can disable this option

Outputs	Description
FQDN (fqdn)	The fully qualified domain name (FQDN)
DNS Provider (dns_provider)	The primary domain of the DNS provider for this domain
Blocklists (blocklists)	An array of strings indicating which blocklist categories this domain is listed on. Current categories are: phishing, malware, spam, anonymizer, nefarious
TLD (tld)	The top-level domain (TLD)
Is Adult (is_adult)	This domain is hosting adult content such as porn, webcams, escorts, etc
Valid (valid)	True if a valid domain was found. For a domain to be considered valid it must be registered and have valid DNS NS records
Is Malicious (is_malicious)	Consider this domain malicious as it is currently listed on at least 1 blocklist
Is Governmental (is_gov)	Is this domain under a government or military TLD
Is Open Network Information Center (is_opennic)	Is this domain under an OpenNIC TLD
Is Subdomain (is_subdomain)	Is the FQDN a subdomain of the primary domain
Registar Name (registrar_name)	The name of the domain registrar owning this domain

NeutrinoAPI/Email Verify method

SMTP based email address verification. Verify real users and filter out low-quality email addresses.Email verify does everything the Email Validate API does but takes validation one step further and performs a realtime SMTP based lookup. This process is similar to how a real email is delivered, so it can verify if an email would actually make it to the recipient address. Our SMTP process will identify if the username exists at the email service provider and can also check if the domain is setup as a catch-all (will accept mail for any address).



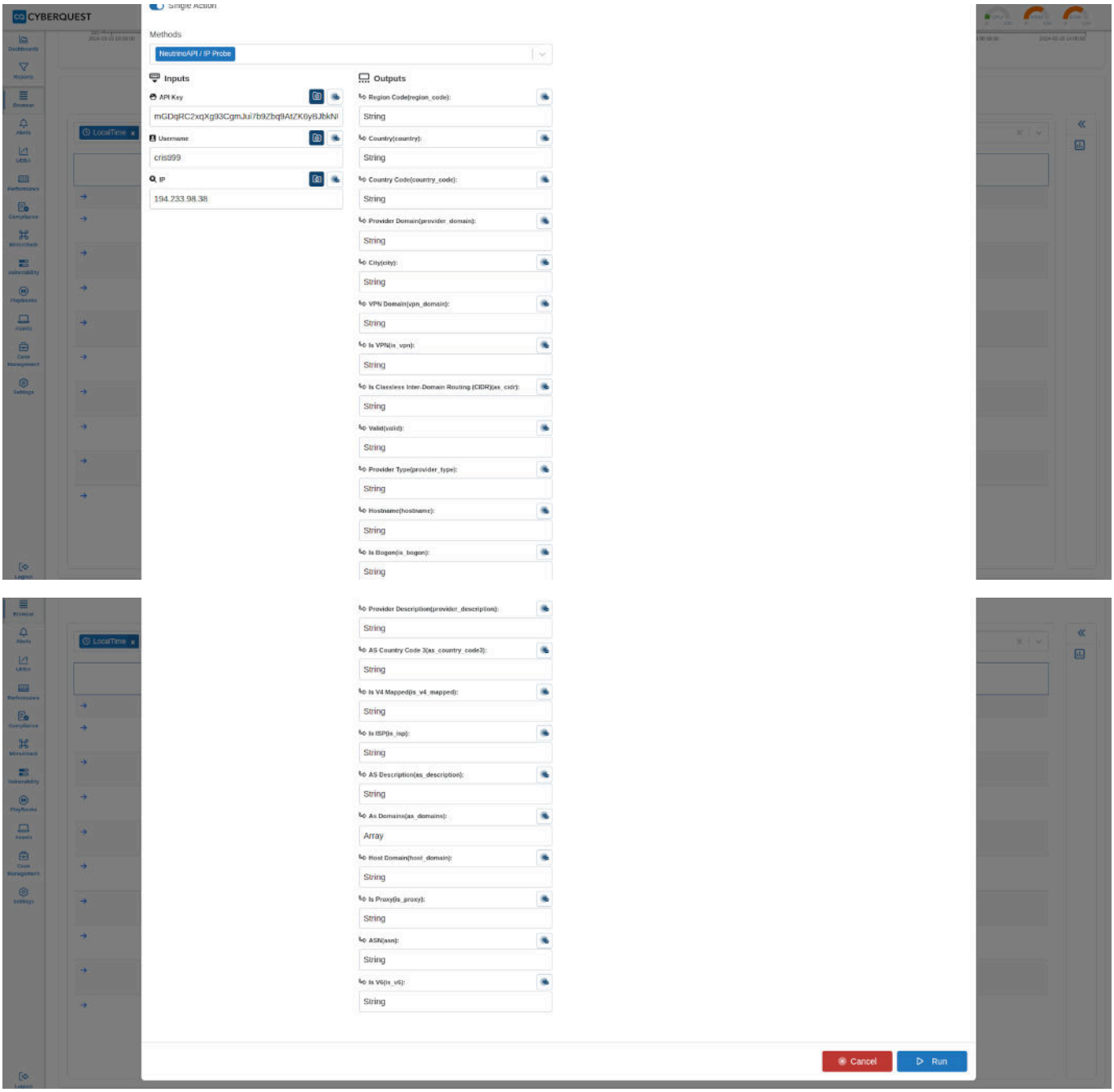


Inputs	Description
API Key (is required)	To use this API you must have an API Key from Neutrino Website
Username (is required)	The username used to Login on Neutrino Website
Email (is required)	An email address
Fix Typos	Automatically attempt to fix typos in the address

Outputs	Description
SMTP Status (smtp_status)	The SMTP username verification status for this address:ok - verification was successful, this is a real username that can receive mailabsent - this username or domain is not registered with the email service providerinvalid - not a valid email address, check the domain-status field for specific detailsunresponsive - the mail servers for this domain have repeatedly timed-out or refused multiple connection attemptsunknown - sorry, we could not reliably determine the status of this username
Typos Fixed (typos_fixed)	True if any typos have been fixed. The fix-typos option must be enabled for this to work
Domain Error (domain_error)	True if this address has any domain name or DNS related errors. Check the domain-status field for the detailed error reason
Verified (verified)	True if this email address has passed SMTP username verification. Check the smtp-status and domain-status fields for specific verification details
Is Free Email (is_freemail)	True if this address is from a free email provider
Is Disposable (is_disposable)	True if this address is a disposable, temporary or darknet related email address
Valid (valid)	Is this a valid email address. To be valid an email must have: correct syntax, a registered and active domain name, correct DNS records and operational MX servers
Is Catch All (is_catch_all)	True if this email domain has a catch-all policy. A catch-all domain will accept mail for any username so therefor the smtp-status will always be ok
Is deferred (is_deferred)	True if the mail server responded with a temporary failure (either a 4xx response code or unresponsive server). You can retry this address later, we recommend waiting at least 15 minutes before retrying
Provider (provider)	The domain name of the email hosting provider
Domain (domain)	The domain name of this email address
SMTP Response (smtp_response)	The raw SMTP response message received during verification
Syntax Error (syntax_error)	True if this address has any syntax errors or is not in RFC compliant formatting
Is Personal (is_personal)	True if this address likely belongs to a person. False if this is a role based address, e.g. admin@, help@, office@, etc.
Email (email)	The complete email address. If you enabled the fix-typos option then this will be the corrected address
MX IP (mx_ip)	The first resolved IP address of the primary MX server, may be empty if there are domain errors present

NeutrinoAPI/IP Probe method

Execute a realtime network probe against an IPv4 or IPv6 address.This API will run a series of live network scans and service probes to extract useful details about the host provider.

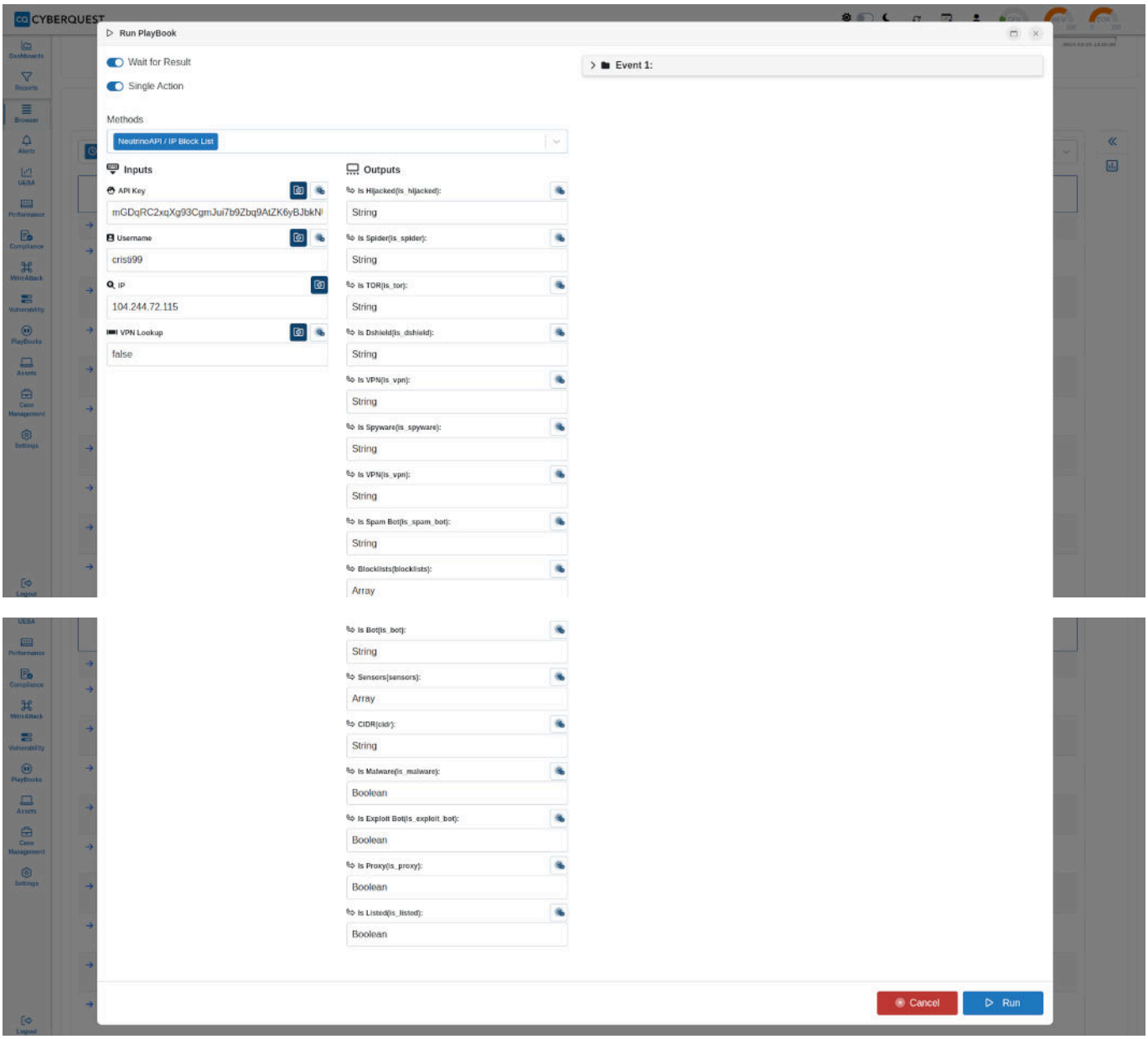


Inputs	Description
API Key (is required)	To use this API you must have an API Key from Neutrino Website
Username (is required)	The username used to Login on Neutrino Website
IP (is required)	IPv4 or IPv6 address

Outputs	Description
Region Code (region_code)	ISO 3166-2 region code (if detectable)
Country (country)	Full country name
Country Code (country_code)	ISO 2-letter country code
Provider Domain (provider_domain)	The domain name of the provider
City (city)	Full city name (if detectable)
VPN Domain (vpn_domain)	The domain of the VPN provider (may be empty if the VPN domain is not detectable)
Is VPN (is_vpn)	True if this IP ia a VPN
Is Classless Inter-Domain Routing (CIDR) (as_cidr)	The autonomous system (AS) CIDR range
Valid (valid)	True if this is a valid IPv4 or IPv6 address
Provider Type (provider_type)	The detected provider type, possible values are:isp - IP belongs to an internet service provider. This includes both mobile, home and business internet providershosting - IP belongs to a hosting company. This includes website hosting, cloud computing platforms and colocation facilitiesvpn - IP belongs to a VPN providerproxy - IP belongs to a proxy service. This includes HTTP/SOCKS proxies and browser based proxiesuniversity - IP belongs to a university/college/campusgovernment - IP belongs to a government department. This includes military facilitiescommercial - IP belongs to a commercial entity such as a corporate headquarters or company officeunknown - could not identify the provider type
Hostname (hostname)	The IPs full hostname (PTR)
Is Bogon (is_bogon)	True if this is a bogon IP address such as a private network, local network or reserved address
Provider Description (provider_description)	A description of the provider (usually extracted from the providers website)
AS Country Code 3 (as_country_code3)	The autonomous system (AS) ISO 3-letter country code
Is V4 Mapped (is_v4_mapped)	True if this is a IPv4 mapped IPv6 address
Is ISP (is_isp)	True if this IP belongs to an internet service provider. Note that this can still be true even if the provider type is VPN/proxy, this occurs in the case that the IP is detected as both types
AS Description (as_description)	The autonomous system (AS) description / company name
As Domains (as_domains)	Array of all the domains associated with the autonomous system (AS)
Host Domain (host_domain)	The IPs host domain
Is Proxy (is_proxy)	True if this IP ia a proxy
ASN (asn)	The autonomous system (AS) number
Is V6 (is_v6)	True if this is a IPv6 address. False if IPv4

NeutrinoAPI/IP Block List method

The IP Blocklist API will detect potentially malicious or dangerous IP addresses.Use this API for identifying malicious hosts, anonymous proxies, tor, botnets, spammers and more.Block, filter or flag traffic to help reduce attacks on your networks and software stacks. IP addresses are automatically removed from the blocklist after 7 days provided no other malicious activity is detected.

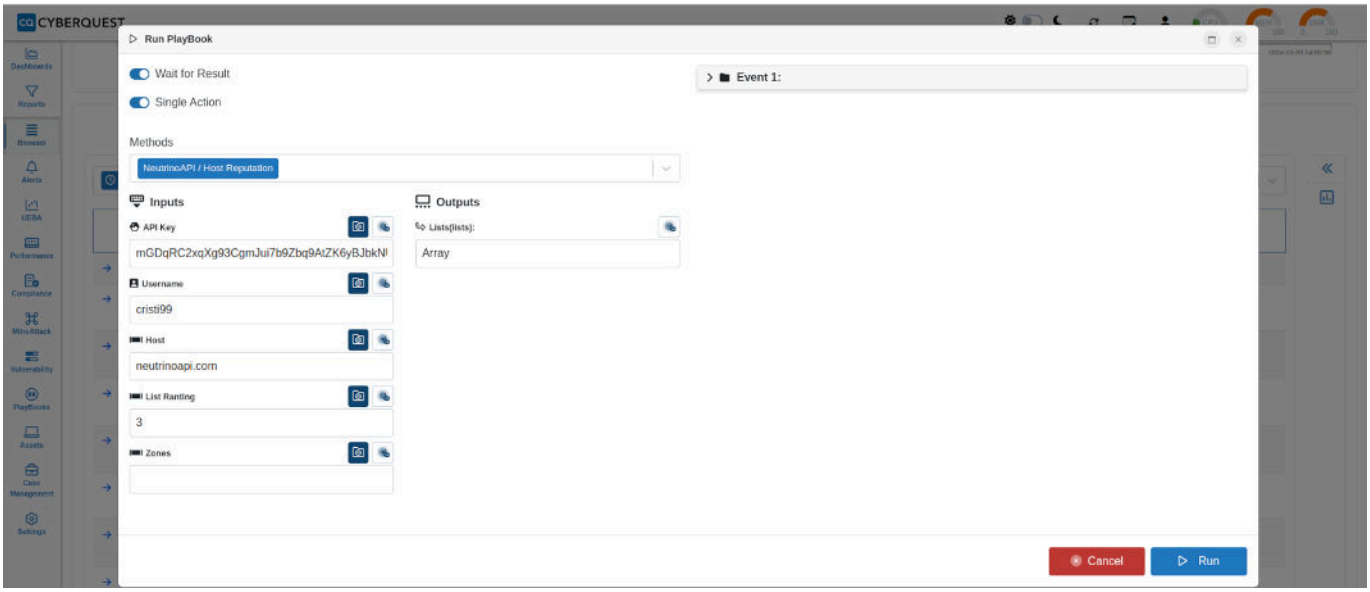


Inputs	Description
API Key (is required)	To use this API you must have an API Key from Neutrino Website
Username (is required)	The username used to Login on Neutrino Website
IP (is required)	
VPN Lookup	Include public VPN provider IP addresses.NOTE: For more advanced VPN detection including the ability to identify private and stealth VPNs use the IP Probe API

Outputs	Description
Is Hijacked (is_hijacked)	IP is part of a hijacked netblock or a netblock controlled by a criminal organization
Is Spider (is_spider)	IP is running a hostile web spider / web crawler
Is TOR (is_tor)	IP is a Tor node or running a Tor related service
Is Dshield (is_dshield)	IP has been flagged as a significant attack source by DShield (dshield.org)
Is VPN (is_vpn)	IP belongs to a public VPN provider (only set if the vpn-lookup option is enabled)
Is Spyware (is_spyware)	IP is involved in distributing or is running spyware
Is VPN (is_vpn)	IP belongs to a public VPN provider (only set if the vpn-lookup option is enabled)
Is Spam Bot (is_spam_bot)	IP address is hosting a spam bot, comment spamming or any other spamming type software
Blocklists (blocklists)	An array of strings indicating which blocklist categories this IP is listed on
Is Bot (is_bot)	IP is hosting a malicious bot or is part of a botnet. This is a broad category which includes brute-force crackers
Sensors (sensors)	An array of objects containing details on which specific sensors detected the IP
CIDR (cidr)	The CIDR address for this listing (only set if the IP is listed)
Is Malware (is_malware)	IP is involved in distributing or is running malware
Is Exploit Bot (is_exploit_bot)	IP is hosting an exploit finding bot or is running exploit scanning software
Is Proxy (is_proxy)	IP has been detected as an anonymous web proxy or anonymous HTTP proxy
Is Listed (is_listed)	Is this IP on a blocklist

NeutrinoAPI/Host Reputation method

Check the reputation of an IP address, domain name or URL against a comprehensive list of blacklists and blocklists.The majority of the lists we check are geared towards filtering hosts involved in the sending or operation of spam however some of the lists are more specialized and will list hosts involved in other forms of cybercrime too. These lists are most commonly known as DNSBLs (Domain Name System Blackhole Lists) or RBLs (Real-time Blackhole Lists) and work using DNS based lookups. All DNSBLs have different listing and removal criteria, if you are trying to delist a host youll need to do this directly with the DNSBL operator. You can usually find more details about an active listing in the txt-record response field. If you want to only check some specific DNSBLs you can supply those using the zones option or you can use the list-rating option to check a range of different lists using our built-in rating system.This API currently checks more than 150 different DNSBLs.

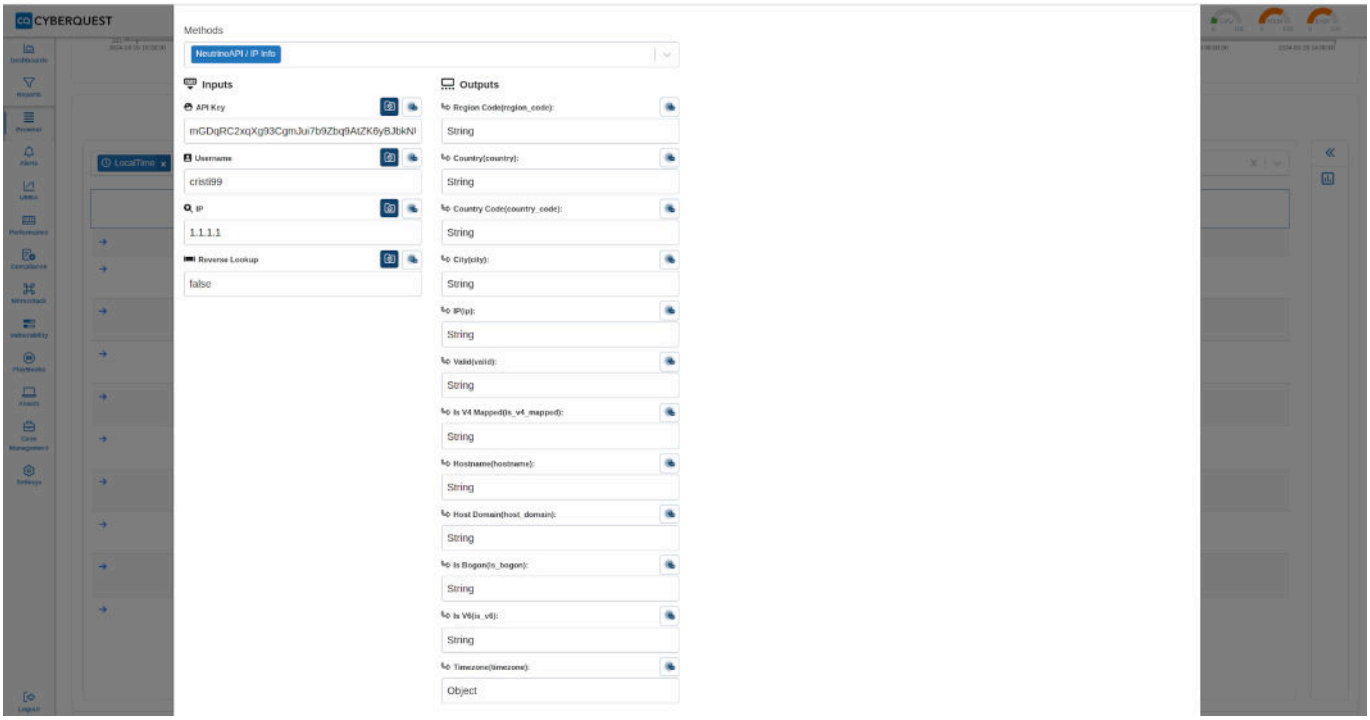


Inputs	Description
API Key (is required)	To use this API you must have an API Key from Neutrino Website
Username (is required)	The username used to Login on Neutrino Website
Host (is required)	An IP address, domain name, FQDN or URL.If you supply a domain/URL it will be checked against the URI DNSBL lists
List Ranting	Only check lists with this rating or better
Zones	Only check these DNSBL zones/hosts. Multiple zones can be supplied as comma-separated values

Outputs	Description
Lists (lists)	Array of objects for each DNSBL (Domain Name System Blacklist)

NeutrinoAPI/IP Info method

Get location information about an IP address and do reverse DNS (PTR) lookups.Identify the geolocation of an IP address down to the city level, including the geographic coordinates (latitude, longitude) and detailed locale information. Our geolocation database is continuously updated in realtime as Internet address allocation changes and as new IP ranges come online. The API supports both IPv4 and IPv6.

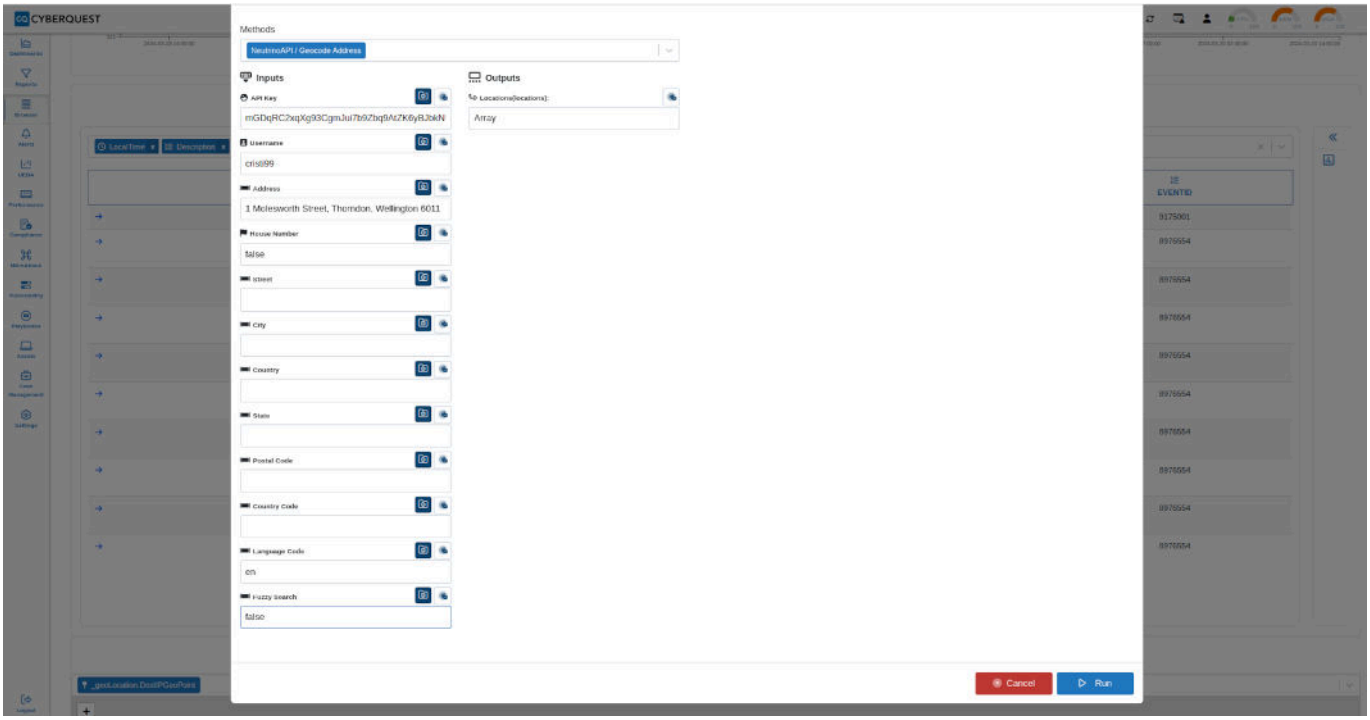


Inputs	Description
API Key (is required)	To use this API you must have an API Key from Neutrino Website
Username (is required)	The username used to Login on Neutrino Website
IP (is required)	IPv4 or IPv6 address
Reverse Lookup	Do a reverse DNS (PTR) lookup. This option can add extra delay to the request so only use it if you need it

Outputs	Description
Region Code (region_code)	ISO 3166-2 region code (if detectable)
Country (country)	Full country name
Country Code (country_code)	ISO 2-letter country code
City (city)	Name of the city (if detectable)
IP (ip)	The IP address
Valid (valid)	True if this is a valid IPv4 or IPv6 address
Is V4 Mapped (is_v4_mapped)	True if this is a IPv4 mapped IPv6 address
Hostname (hostname)	The IPs full hostname (only set if reverse-lookup has been used)
Host Domain (host_domain)	The IPs host domain (only set if reverse-lookup has been used)
Is Bogon (is_bogon)	True if this is a bogon IP address such as a private network, local network or reserved address
Is V6 (is_v6)	True if this is a IPv6 address. False if IPv4
Timezone (timezone)	Map containing timezone details for the location

NeutrinoAPI/Geocode Address method

Geocode an address, partial address or just the name of a place.Address geocoding is the process of taking a string and attempting to match this with possible real world locations. This is the opposite process of reverse geocoding. Once a location is found you can then retrieve the geographic coordinates as latitude and longitude. If more than one location is found for a given string then results are ordered by most relevant to the original search address and with the highest geographic accuracy.

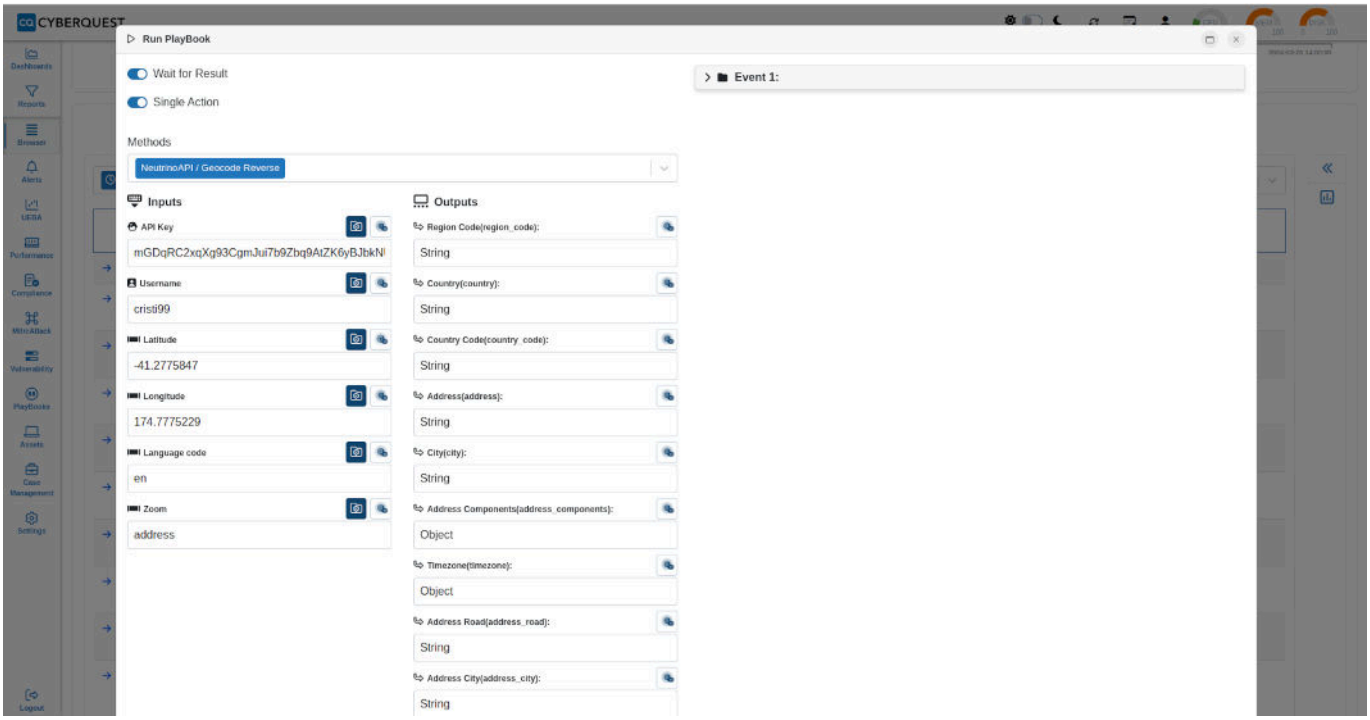


Inputs	Description
API Key (is required)	To use this API you must have an API Key from Neutrino Website
Username (is required)	The username used to Login on Neutrino Website
Address	The full address, partial address or name of a place to try and locate. Comma separated address components are preferred.
House Number	The house/building number to locate
Street	The street/road name to locate
City	The city/town name to locate
Country	The county/region name to locate
State	The state name to locate
Postal Code	The postal code to locate
Country Code	Limit result to this country (the default is no country bias)
Language Code	The language to display results in, available languages are:de, en, es, fr, it, pt, ru, zh
Fuzzy Search	If no matches are found for the given address, start performing a recursive fuzzy search until a geolocation is found. This option is recommended for processing user input or implementing auto-complete. We use a combination of approximate string matching and data cleansing to find possible location matches

Outputs	Description
Locations (locations)	A list of locations that meet the search criteria

NeutrinoAPI/Geocode Reverse method

Convert a geographic coordinate (latitude and longitude) into a real world address.This API is ideal for applications which process raw location data like coordinates obtained from mobile GPS devices. Reverse geocoding is the opposite process of address geocoding, you can get detailed location data right down to a specific building or zoomed out to the street, city or country level.

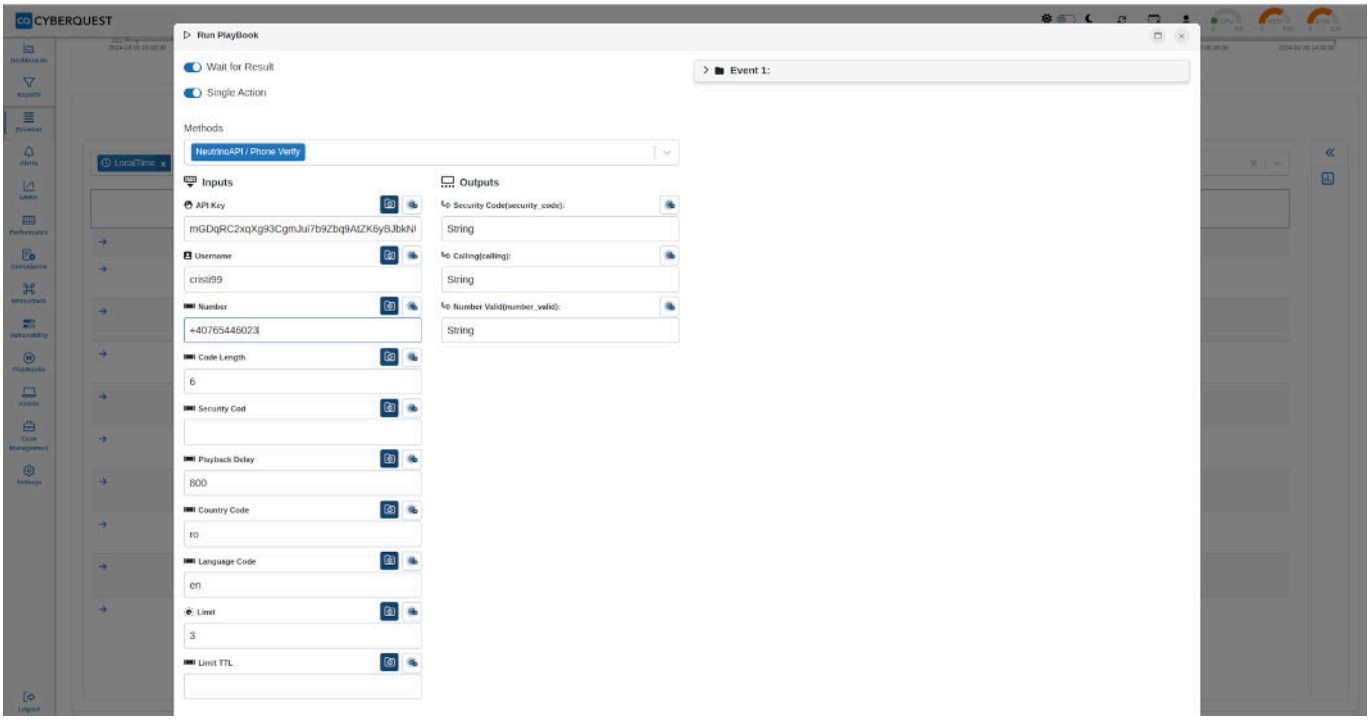


Inputs	Description
API Key (is required)	To use this API you must have an API Key from Neutrino Website
Username (is required)	The username used to Login on Neutrino Website
Latitude (is required)	The location latitude in decimal degrees format
Longitude (is required)	The location longitude in decimal degrees format
Language code	The language to display results in, available languages are:de, en, es, fr, it, pt, ru
Zoom	The zoom level to respond with:address - the most precise address availablestreet - the street levelcity - the city levelstate - the state levelcountry - the country level

Outputs	Description
Region Code (region_code)	The ISO 3166-2 region code for the location
Country (country)	The country of the location
Country Code (country_code)	The ISO 2-letter country code of the location
Address (address)	The complete address using comma-separated values
City (city)	The city of the location
Address Components (address_components)	The components which make up the address such as road, city, state, etc
Timezone (timezone)	Map containing timezone details for the location:
Address Road (address_road)	Component which make up the address: road
Address City (address_city)	Component which make up the address: city
Address Country (address_county)	Component which make up the address: country
Address Suburban (address_suburb)	Component which make up the address: suburb
House Number (address_house_number)	Component which make up the address: house number
Postal Code (postal_code)	The postal code for the location
Found (found)	True if these coordinates map to a real location

NeutrinoAPI/Phone Verify method

Make an automated call to any valid phone number and playback a unique security code.Use this API to verify personal details, help reduce fraud and in authentication systems for implementing multi-factor (MFA and 2FA) authentication. Supply your own security code for use in TOTP systems (the most common standard for 2FA implementations) or let us auto generate a secure random code. To then verify a delivered code you can either implement this on your side or use use the verify security code endpoint.

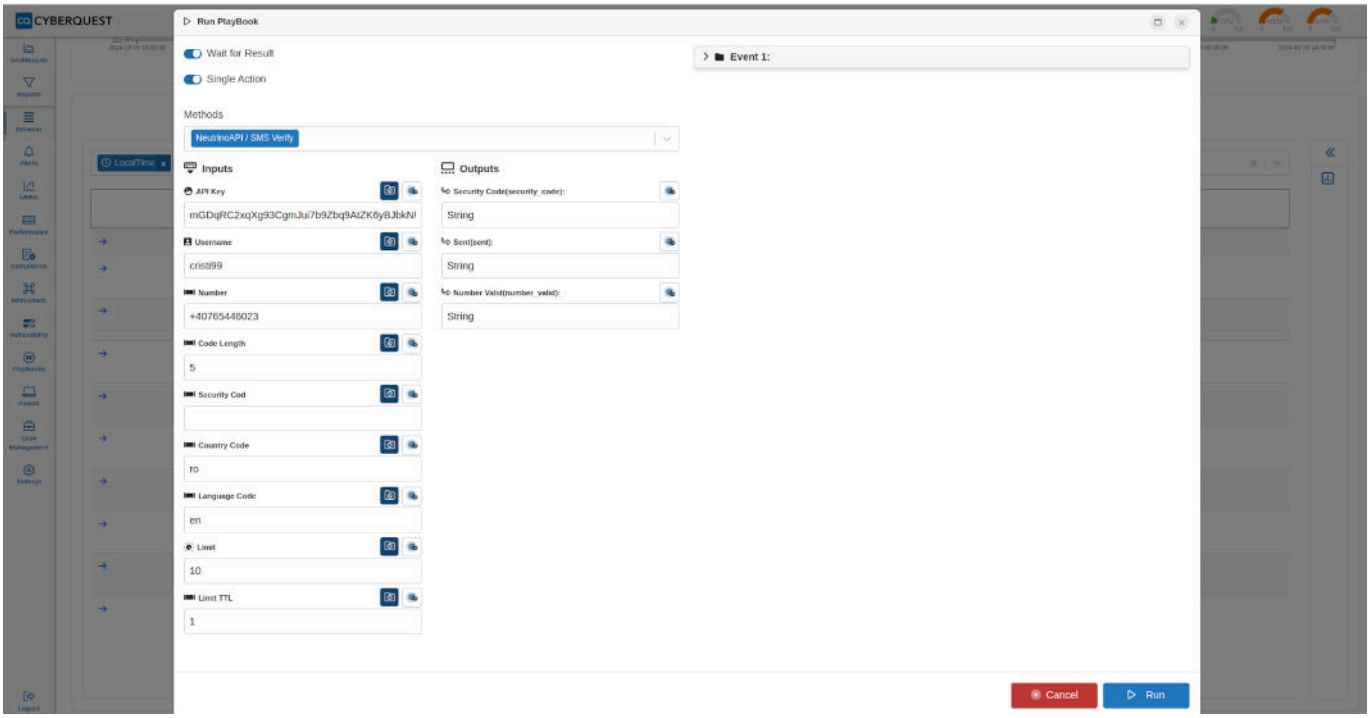


Inputs	Description
API Key (is required)	To use this API you must have an API Key from Neutrino Website
Username (is required)	The username used to Login on Neutrino Website
Number (is required)	The phone number to send the verification code to
Code Length	The number of digits to use in the security code (between 4 and 12)
Security Cod	Pass in your own security code. This is useful if you have implemented TOTP or similar 2FA methods. If not set then we will generate a secure random code
Playback Delay	The delay in milliseconds between the playback of each security code
Country Code	ISO 2-letter country code, assume numbers are based in this country.If not set numbers are assumed to be in international format (with or without the leading + sign)
Language Code	The language to playback the verification code in, available languages are:de - Germanen - Englishes - Spanishfr - Frenchit - Italianpt - Portugueseru - Russian
Limit	Limit the total number of calls allowed to the supplied phone number, if the limit is reached within the TTL then error code 14 will be returned
Limit TTL	Set the TTL in number of days that the limit option will remember a phone number (the default is 1 day and the maximum is 365 days)

Outputs	Description
Security Code (security_code)	The security code generated, you can save this code to perform your own verification or you can use the Verify Security Code API
Calling (calling)	True if the call is being made now
Number Valid (number_valid)	The security code generated, you can save this code to perform your own verification or you can use the Verify Security Code API

NeutrinoAPI/SMS Verify method

Send a unique security code to any mobile device via SMS.Use this API to verify personal details, help reduce fraud and in authentication systems for implementing multi-factor (MFA and 2FA) authentication. Supply your own security code for use in TOTP (the most common standard for 2FA implementations) or let us auto generate a secure random code. To then verify a delivered code you can either implement this on your side or use use the verify security code endpoint.

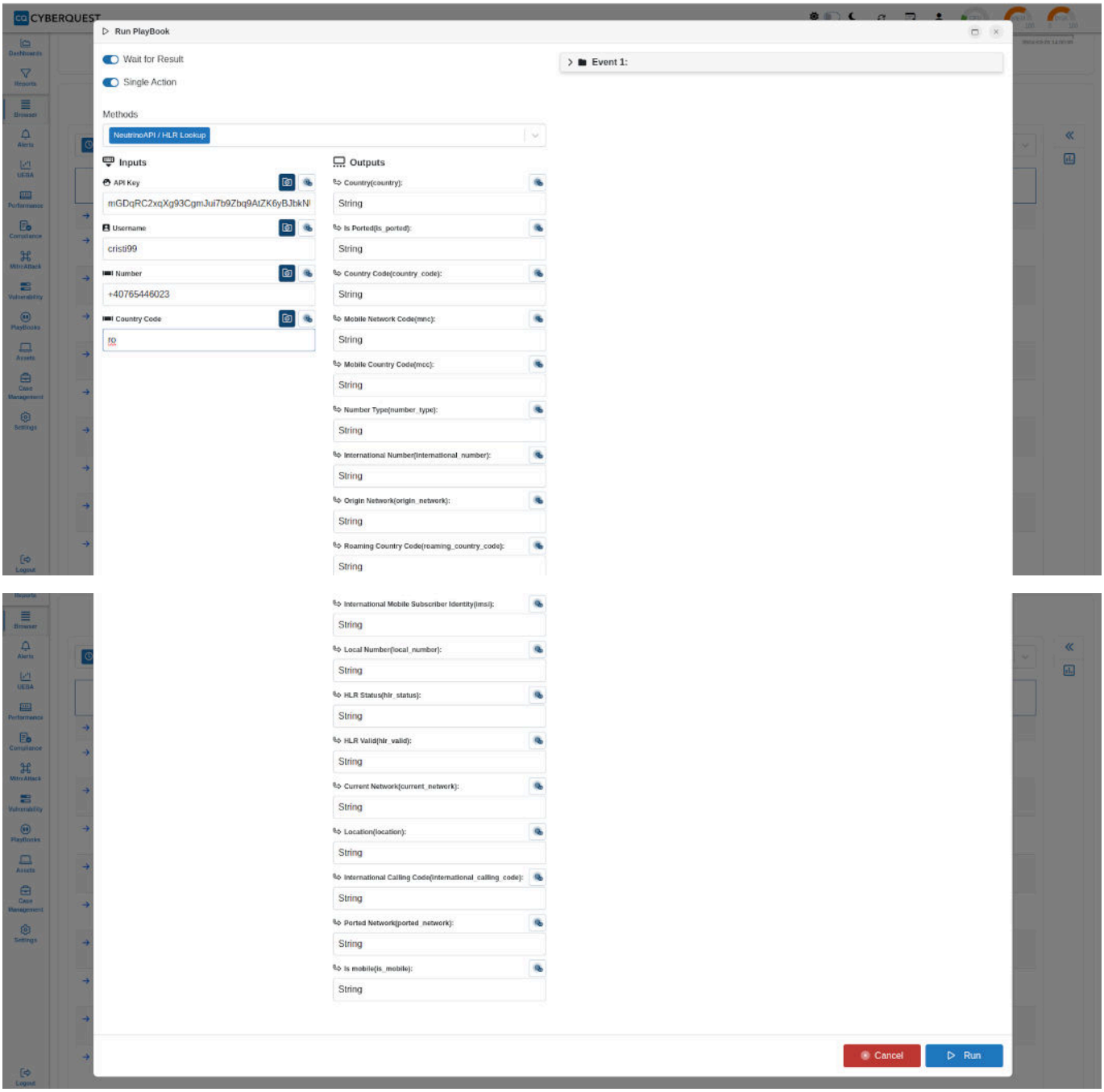


Inputs	Description
API Key (is required)	To use this API you must have an API Key from Neutrino Website
Username (is required)	The username used to Login on Neutrino Website
Number (is required)	The phone number to send a verification code to
Code Length	The number of digits to use in the security code (must be between 4 and 12)
Security Cod	Pass in your own security code. This is useful if you have implemented TOTP or similar 2FA methods. If not set then we will generate a secure random code
Country Code	ISO 2-letter country code, assume numbers are based in this country.If not set numbers are assumed to be in international format (with or without the leading + sign)
Language Code	The language to send the verification code in, available languages are:de - Germanen - Englishes - Spanishfr - Frenchit - Italianpt - Portugueseru - Russian
Limit	Limit the total number of SMS allowed to the supplied phone number, if the limit is reached within the TTL then error code 14 will be returned
Limit TTL	Set the TTL in number of days that the limit option will remember a phone number (the default is 1 day and the maximum is 365 days)

Outputs	Description
Security Code (security_code)	The security code generated, you can save this code to perform your own verification or you can use the Verify Security Code API
Sent (sent)	True if the SMS has been sen
Number Valid (number_valid)	True if this a valid phone number

NeutrinoAPI/HLR Lookup method

Connect to the global mobile cellular network and retrieve the status of a mobile device.The home location register (HLR) is a central database that contains details of each mobile phone subscriber connected to the global mobile network. You can use this API to validate that a mobile number is live and registered on a mobile network in real-time. Find out the carrier name, ported number status and fetch up-to-date device status.

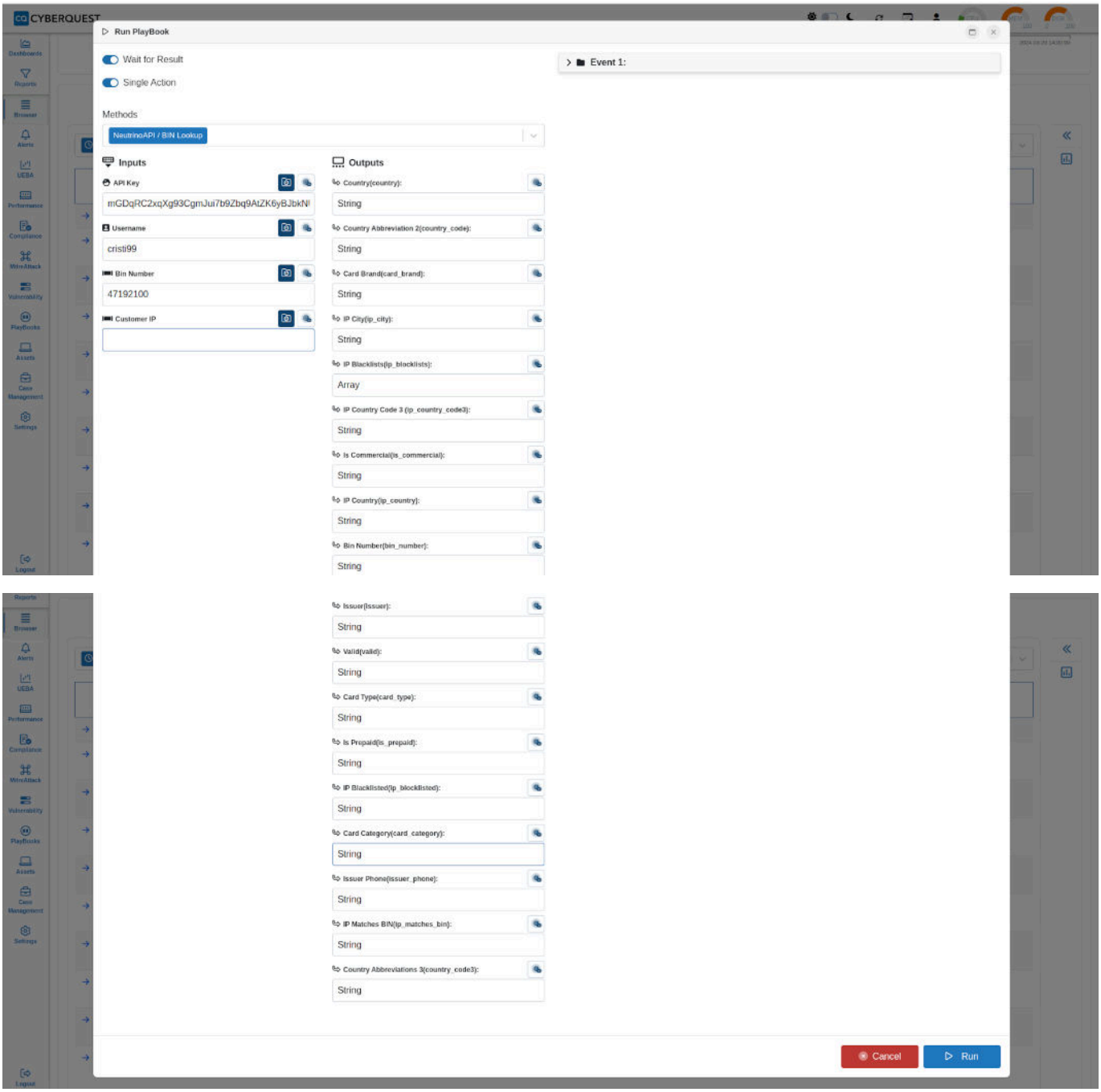


Inputs	Description
API Key (is required)	To use this API you must have an API Key from Neutrino Website
Username (is required)	The username used to Login on Neutrino Website
Number (is required)	A phone number
Country Code	ISO 2-letter country code, assume numbers are based in this country.If not set numbers are assumed to be in international format (with or without the leading + sign)

Outputs	Description
Country (country)	The phone number country
Is Ported (is_ported)	Has this number been ported to another network
Country Code (country_code)	ISO 4217 currency code associated with the country
Mobile Network Code (mnc)	The mobile MNC number (Mobile Network Code)
Mobile Country Code (mcc)	The mobile MCC number (Mobile Country Code)
Number Type (number_type)	The number type, possible values are:mobilefixed-linepremium-ratetoll-freevoipunknown
International Number (international_number)	The number represented in full international format
Origin Network (origin_network)	The origin network/carrier name
Roaming Country Code (roaming_country_code)	If the number is currently roaming, the ISO 2-letter country code of the roaming in country
International Mobile Subscriber Identity (imsi)	The mobile IMSI number (International Mobile Subscriber Identity)
Local Number (local_number)	The number represented in local dialing format
HLR Status (hlr_status)	The HLR lookup status, possible values are:ok - the HLR lookup was successful and the device is connectedabsent - the number was once registered but the device has been switched off or out of network range for some timeunknown - the number is not known by the mobile networkinvalid - the number is not a valid mobile MSISDN numberfixed-line - the number is a registered fixed-line not mobilevoip - the number has been detected as a VOIP linefailed - the HLR lookup has failed, we could not determine the real status of this number
HLR Valid (hlr_valid)	Was the HLR lookup successful. If true then this is a working and registered cell-phone or mobile device (SMS and phone calls will be delivered)
Current Network (current_network)	The currently used network/carrier name
Location (location)	The number location. Could be a city, region or country depending on the type of number
International Calling Code (international_calling_code)	The international calling code
Ported Network (ported_network)	The ported to network/carrier name (only set if the number has been ported)
Is mobile (is_mobile)	True if this is a mobile number (only true with 100% certainty, if the number type is unknown this value will be false)

NeutrinoAPI/BIN Lookup method

Parse, validate and get detailed user-agent information from a user agent string or from client hints.

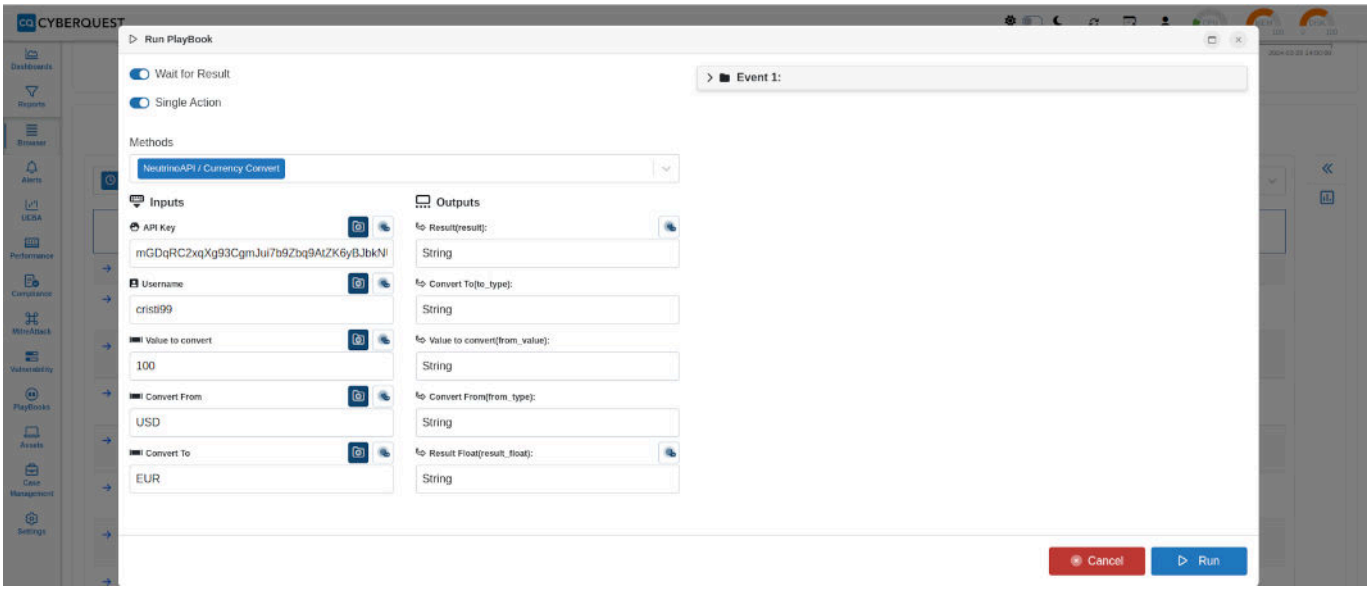


Inputs	Description
API Key (is required)	To use this API you must have an API Key from Neutrino Website
Username (is required)	The username used to Login on Neutrino Website
Bin Number	The BIN or IIN number. This is the first 6, 8 or 10 digits of a card number, use 8 (or more) digits for the highest level of accuracy
Customer IP	Pass in the customers IP address and we will return some extra information about them

Outputs	Description
Country (country)	The full country name of the issuer
Country Abbreviation 2 (country_code)	The ISO 2-letter country code of the issuer
Card Brand (card_brand)	The card brand (e.g. Visa or Mastercard)
IP City (ip_city)	The city of the customers IP (if detectable)
IP Blacklists (ip_blocklists)	An array of strings indicating which blocklists this IP is listed on
IP Country Code 3 (ip_country_code3)	The ISO 3-letter country code of the customers IP
Is Commercial (is_commercial)	Is this a commercial/business use card
IP Country (ip_country)	The country of the customers IP
Bin Number (bin_number)	The BIN or IIN number
Issuer (issuer)	The card issuer
Valid (valid)	Is this a valid BIN or IIN number
Card Type (card_type)	The card type, will always be one of: DEBIT, CREDIT, CHARGE CARD
Is Prepaid (is_prepaid)	Is this a prepaid or prepaid reloadable card
IP Blacklisted (ip_blocklisted)	True if the customers IP is listed on one of our blocklists
Card Category (card_category)	The card category. There are many different card categories the most common card categories are: CLASSIC, BUSINESS, CORPORATE, PLATINUM, PREPAID
Issuer Phone (issuer_phone)	The card issuers phone number
IP Matches BIN (ip_matches_bin)	True if the customers IP country matches the BIN country
Country Abbreviations 3 (country_code3)	The ISO 3-letter country code of the issuer

NeutrinoAPI/Currency Convert method

A currency and unit conversion tool.Convert between currency, cryptocurrency and various other units using an up-to-date data feed.All major currencies are updated every 15 minutes with exchange rates aggregated from multiple international exchanges and averaged out.

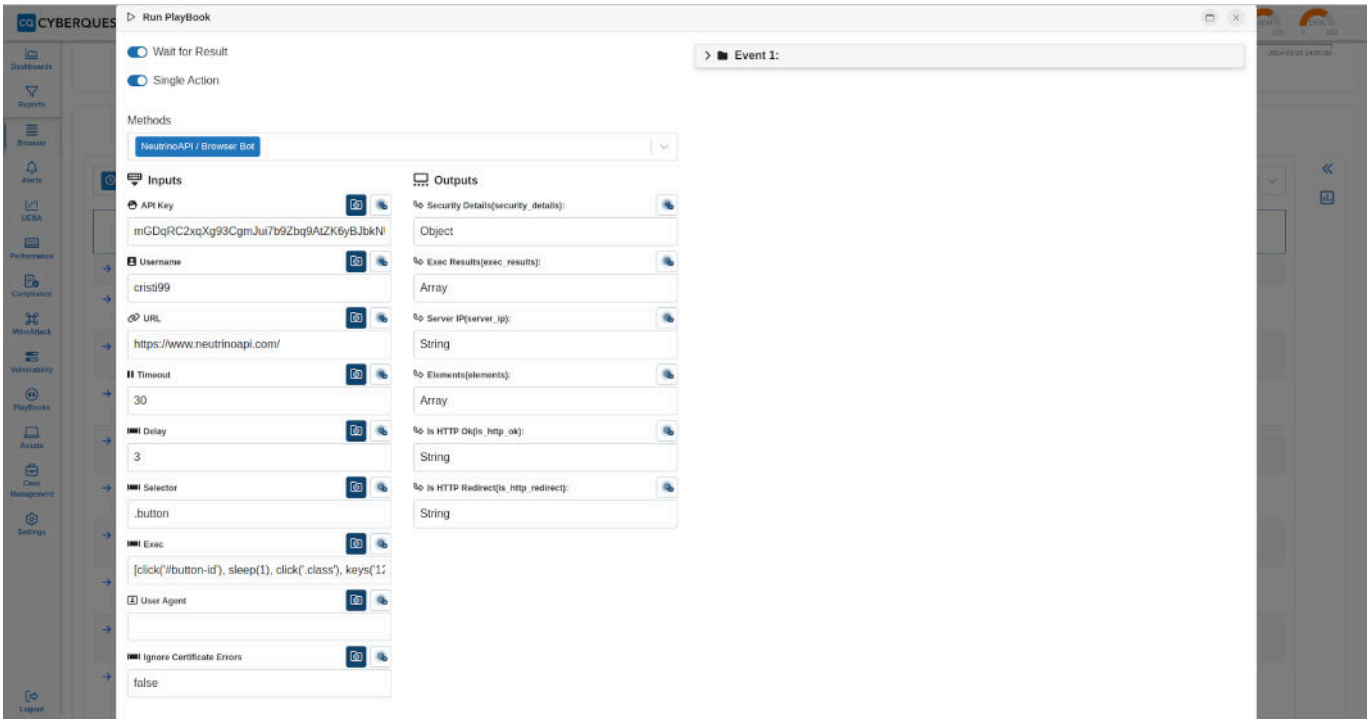


Inputs	Description
API Key (is required)	To use this API you must have an API Key from Neutrino Website
Username (is required)	The username used to Login on Neutrino Website
Value to convert (is required)	The value to convert from (e.g. 10.95)
Convert From	The type of the value to convert from (e.g. USD)
Convert To	The type to convert to (e.g. EUR)

Outputs	Description
Result (result)	The result of the conversion in string format
Convert To (to_type)	
Value to convert (from_value)	
Convert From (from_type)	
Result Float (result_float)	The result of the conversion as a floating-point number

NeutrinoAPI/Browser Bot method

Parse, validate and get detailed user-agent information from a user agent string or from client hints.

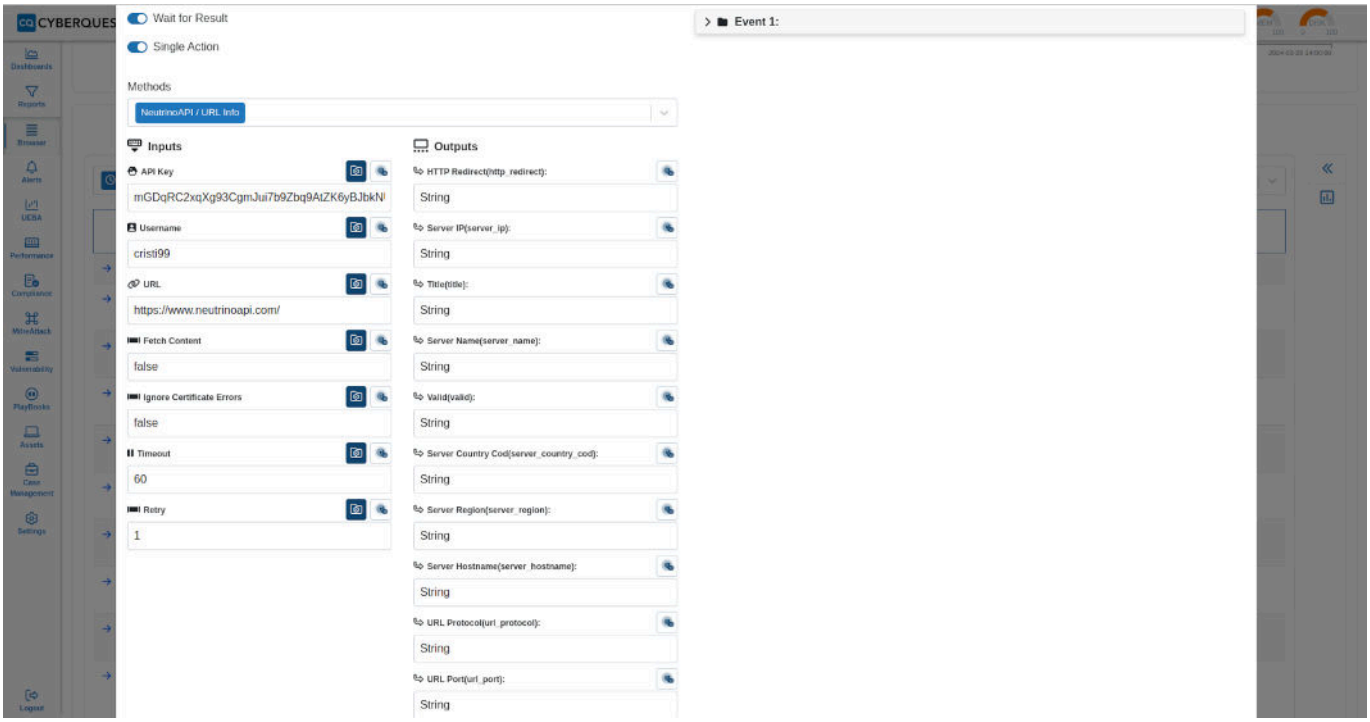


Inputs	Description
API Key (is required)	To use this API you must have an API Key from Neutrino Website
Username (is required)	The username used to Login on Neutrino Website
URL (is required)	The URL to load
Timeout	Timeout in seconds. Give up if still trying to load the page after this number of seconds
Delay	Delay in seconds to wait before capturing any page data, executing selectors or JavaScript
Selector	Extract content from the page DOM using this selector. Commonly known as a CSS selector
Exec	Execute JavaScript on the website. This parameter accepts JavaScript as either a string containing JavaScript or for sending multiple separate statements a JSON array or POST array can also be used. If a statement returns any value it will be returned in the exec-results response. You can also use the following specially defined user interaction functions:sleep(seconds); Just wait/sleep for the specified number of seconds.click(selector); Click on the first element matching the given selector.focus(selector); Focus on the first element matching the given selector.keys(characters); Send the specified keyboard characters. Use click() or focus() first to send keys to a specific element.enter(); Send the Enter key.tab(); Send the Tab key.
User Agent	Override the browsers default user-agent string with this one
Ignore Certificate Errors	Ignore any TLS/SSL certificate errors and load the page anyway

Outputs	Description
Security Details (security_details)	Map containing details of the TLS/SSL setup
Exec Results (exec_results)	If you executed any JavaScript this array holds the results as objects
Server IP (server_ip)	The HTTP servers IP address
Elements (elements)	Array containing all the elements matching the supplied selector.Each element object will contain the text content, HTML content and all current element attributes
Is HTTP Ok (is_http_ok)	True if the HTTP status is OK (200)
Is HTTP Redirect (is_http_redirect)	True if the URL responded with an HTTP redirect

NeutrinoAPI/URL Info method

Parse, analyze and retrieve content from the supplied URL.Determine if a URL is well-formed and actually hosting real content. Determine many of the URLs properties such as its current HTTP status, content size, type, encoding and load time. You can also use this API to fetch the actual URL response data for further processing or storage.

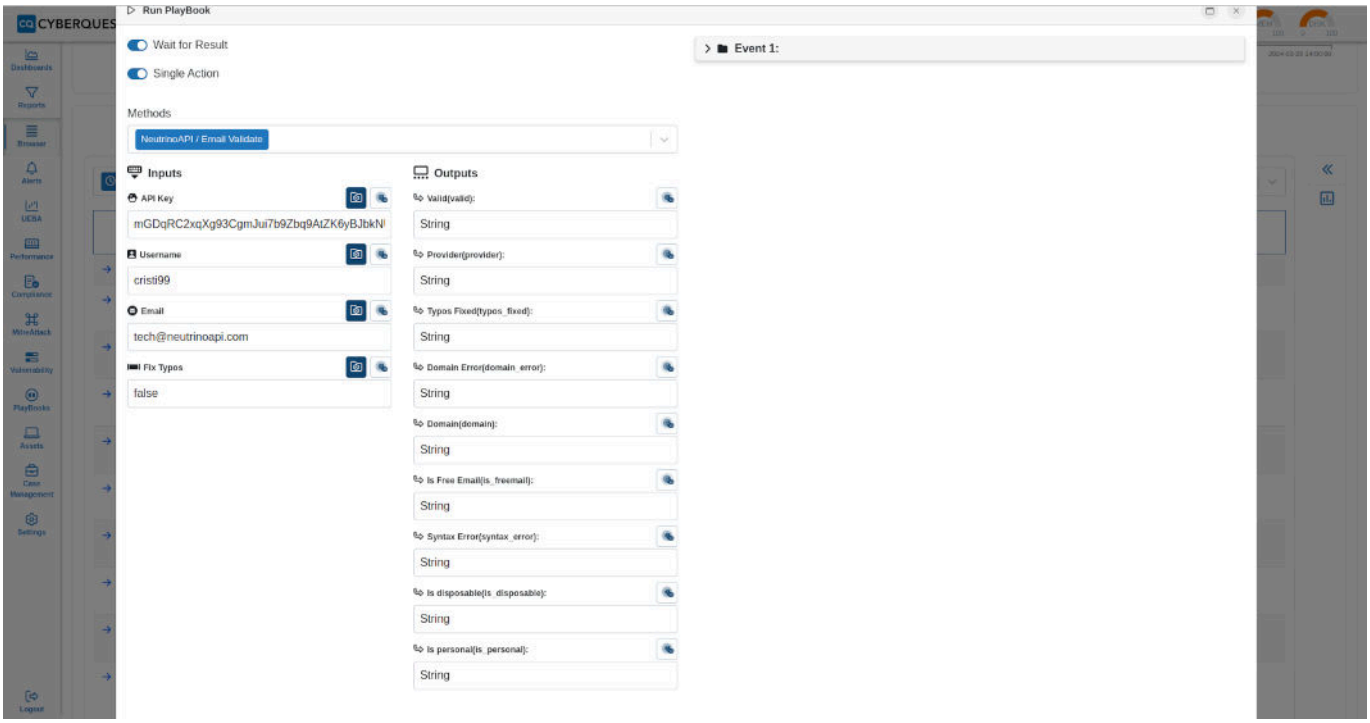


Inputs	Description
API Key (is required)	To use this API you must have an API Key from Neutrino Website
Username (is required)	The username used to Login on Neutrino Website
URL (is required)	The URL to probe
Fetch Content	If this URL responds with html, text, json or xml then return the response. This option is useful if you want to perform further processing on the URL content (e.g. with the HTML Extract or HTML Clean APIs)
Ignore Certificate Errors	Ignore any TLS/SSL certificate errors and load the URL anyway
Timeout	Timeout in seconds. Give up if still trying to load the URL after this number of seconds
Retry	If the request fails for any reason try again this many times

Outputs	Description
HTTP Redirect (http_redirect)	True if this URL responded with an HTTP redirect
Server IP (server_ip)	True if this URL responded with an HTTP redirect
Title (title)	The document title
Server Name (server_name)	The name of the server software hosting this URL
Valid (valid)	Is this a valid well-formed URL
Server Country Cod (server_country_cod)	The servers IP geo-location: ISO 2-letter country code
Server Region (server_region)	The servers IP geo-location: full region name (if detectable)
Server Hostname (server_hostname)	The servers hostname (PTR record)
URL Protocol (url_protocol)	The URL protocol, usually http or https
URL Port (url_port)	The URL port

NeutrinoAPI/Email Validate method

Parse, validate and clean an email address.

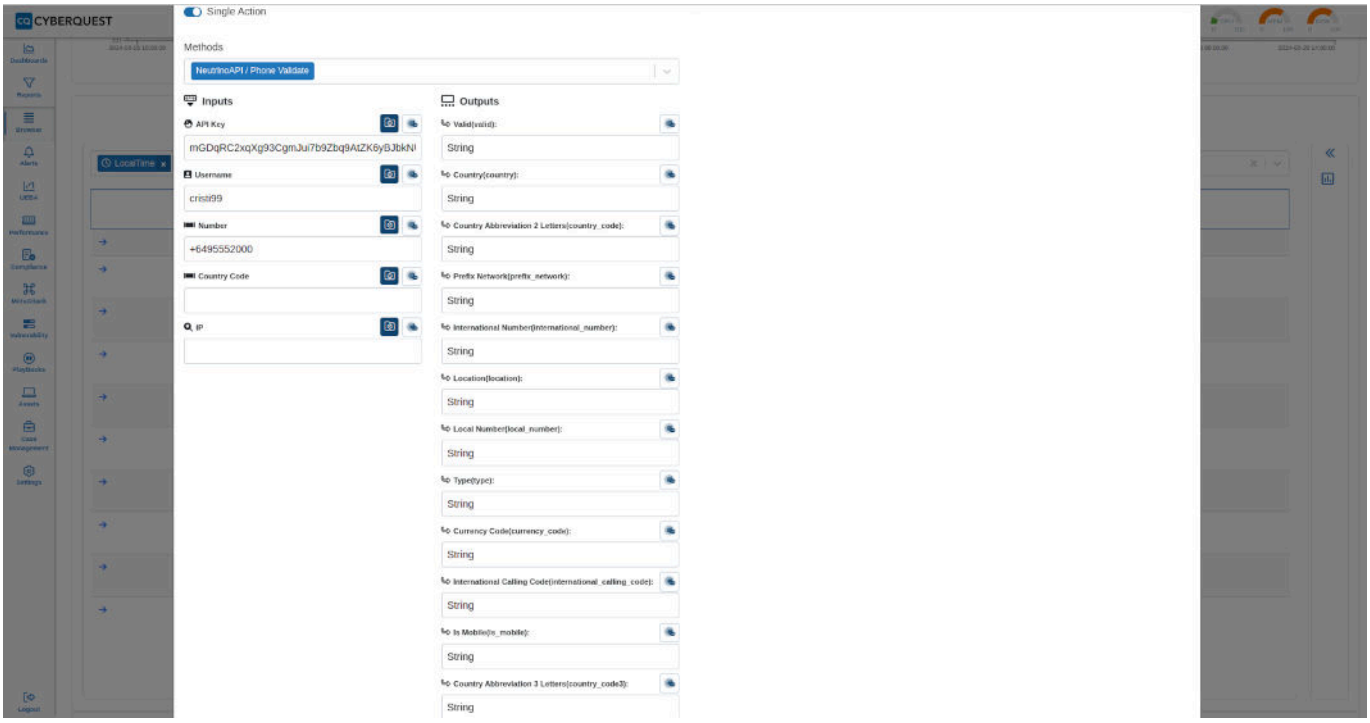


Inputs	Description
API Key (is required)	To use this API you must have an API Key from Neutrino Website
Username (is required)	The username used to Login on Neutrino Website
Email (is required)	An email address
Fix Typos	Automatically attempt to fix typos in the address

Outputs	Description
Valid (valid)	Is this a valid email address. To be valid an email must have: correct syntax, a registered and active domain name, correct DNS records and operational MX servers
Provider (provider)	The domain name of the email hosting provider
Typos Fixed (typos_fixed)	The complete email address. If you enabled the fix-typos option then this will be the corrected address
Domain Error (domain_error)	True if this address has any domain name or DNS related errors. Check the domain-status field for the detailed error reason
Domain (domain)	The domain name of this email address
Is Free Email (is_freemail)	True if this address is from a free email provider
Syntax Error (syntax_error)	True if this address has any syntax errors or is not in RFC compliant formatting
Is disposable (is_disposable)	True if this address is a disposable, temporary or darknet related email address
Is personal (is_personal)	True if this address likely belongs to a person. False if this is a role based address, e.g. admin@, help@, office@, etc.

NeutrinoAPI/Phone Validate method

Parse, validate and get location information about a phone number.

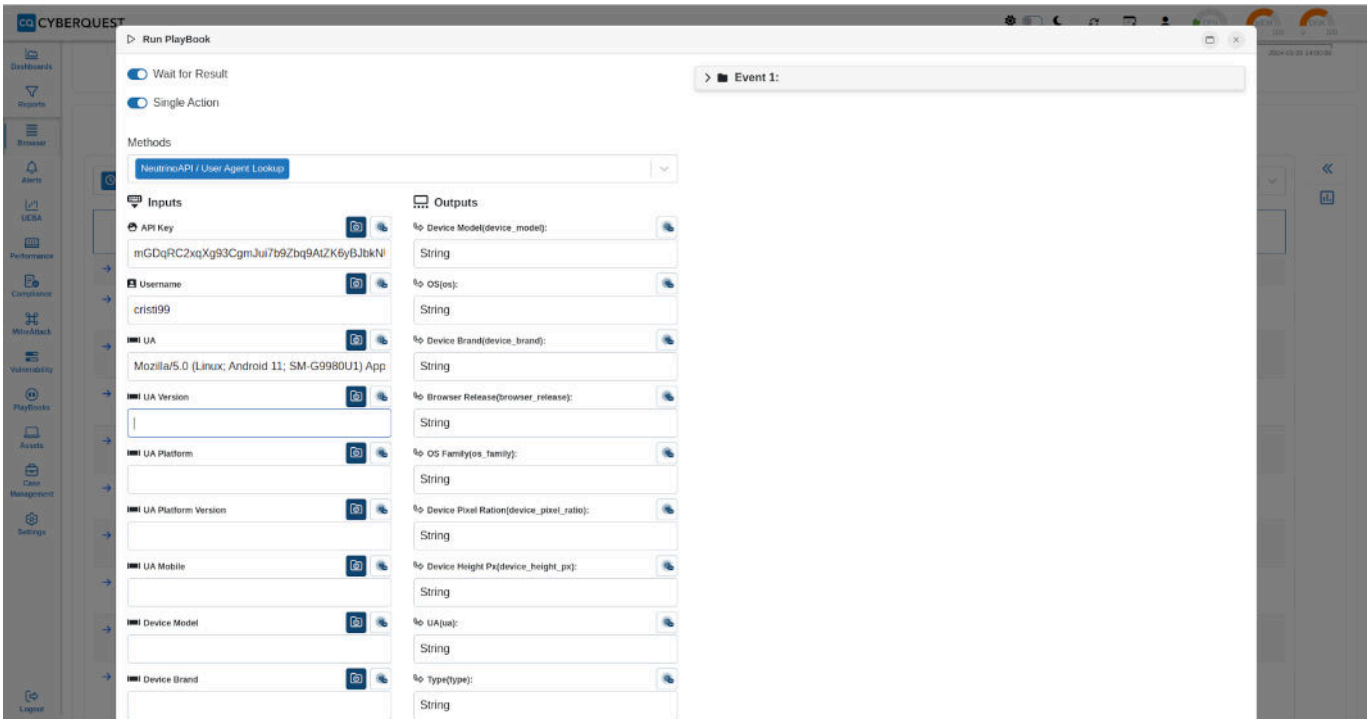


Inputs	Description
API Key (is required)	To use this API you must have an API Key from Neutrino Website
Username (is required)	The username used to Login on Neutrino Website
Number (is required)	A phone number. This can be in international format (E.164) or local format. If passing local format you must also set either the country-code OR ip options as well
Country Code	ISO 2-letter country code, assume numbers are based in this country. If not set numbers are assumed to be in international format (with or without the leading + sign)
IP	Pass in a users IP address and we will assume numbers are based in the country of the IP address

Outputs	Description
Valid (valid)	Is this a valid phone number
Country (country)	The phone number country
Country Abbreviation 2 Letters (country_code)	The phone number country as an ISO 2-letter country code
Prefix Network (prefix_network)	The network/carrier who owns the prefix (this only works for some countries, use HLR lookup for global network detection)
International Number (international_number)	The number represented in full international format (E.164)
Location (location)	The phone number location. Could be the city, region or country depending on the type of number
Local Number (local_number)	The number represented in local dialing format
Type (type)	The number type based on the number prefix.Possible values are:mobilefixed-linepremium-ratetoll-freevoipunknown (use HLR lookup)
Currency Code (currency_code)	ISO 4217 currency code associated with the country
International Calling Code (international_calling_code)	The international calling code
Is Mobile (is_mobile)	True if this is a mobile number. If the number type is unknown this value will be false
Country Abbreviation 3 Letters (country_code3)	The phone number country as an ISO 3-letter country code

NeutrinoAPI/User Agent Lookup method

Parse, validate and get detailed user-agent information from a user agent string or from client hints.

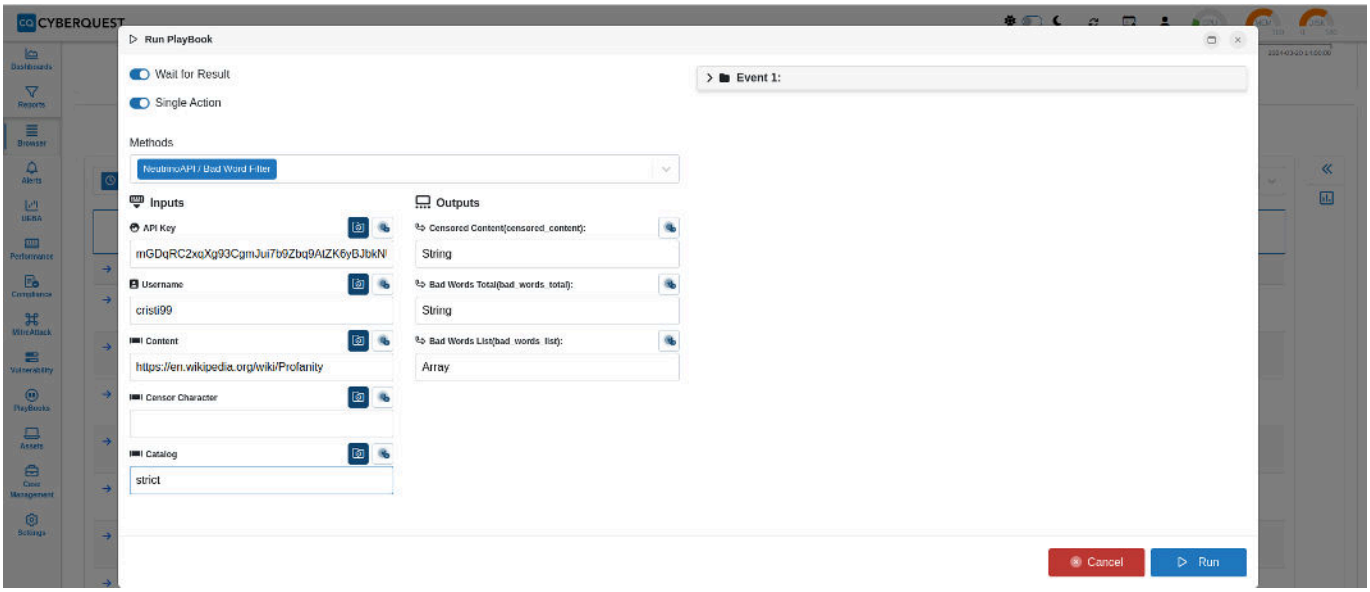


Inputs	Description
API Key (is required)	To use this API you must have an API Key from Neutrino Website
Username (is required)	The username used to Login on Neutrino Website
UA (is required)	The user-agent string to lookup. For client hints use the UA header or the JSON data directly from navigator.userAgentData.brands or navigator.userAgentData.getHighEntropyValues()
UA Version	For client hints this corresponds to the UA-Full-Version header or uaFullVersion from NavigatorUAData
UA Platform	For client hints this corresponds to the UA-Platform header or platform from NavigatorUAData
UA Platform Version	For client hints this corresponds to the UA-Platform-Version header or platformVersion from NavigatorUAData
UA Mobile	For client hints this corresponds to the UA-Mobile header or mobile from NavigatorUAData
Device Model	For client hints this corresponds to the UA-Model header or model from NavigatorUAData.You can also use this parameter to lookup a device directly by its model name, model code or hardware code, on android you can get the model name from: https://developer.android.com/reference/android/os/Build.html#MODEL (https://developer.android.com/reference/android/os/Build.html#MODEL)
Device Brand	This parameter is only used in combination with device-model when doing direct device lookups without any user-agent data. Set this to the brand or manufacturer name, this is required for accurate device detection with ambiguous model names. On android you can get the device brand from: https://developer.android.com/reference/android/os/Build#MANUFACTURER (https://developer.android.com/reference/android/os/Build#MANUFACTURER)

Outputs	Description
Device Model (device_model)	The device model
OS (os)	The full operating system name
Device Brand (device_brand)	The device brand / manufacturer
Browser Release (browser_release)	If the client is a web browser which year was this browser version released
OS Family (os_family)	The operating system family. The major OS families are: Android, Windows, macOS, iOS, Linux
Device Pixel Ration (device_pixel_ratio)	The device display pixel ratio (the ratio of the resolution in physical pixels to the resolution in CSS pixels)
Device Height Px (device_height_px)	The device display height in CSS px
UA (ua)	The user agent string
Type (type)	The user agent type, possible values are:desktopphonetabletwearabletvconsoleemaillibraryrobotunknown
Device PPI (device_ppi)	The device display PPI (pixels per inch)
Version (version)	The client software full version
Version Major (version_major)	The client software major version
OS Version Major (os_version_major)	The operating system major version
Browser Engine (browser_engine)	If the client is a web browser which underlying browser engine does it use
Device Model Code (device_model_code)	The device model code
OS Version (os_version)	The operating system full version
Device Release (device_release)	The year when this device model was released
Name (name)	The client software name
Is Webview (is_webview)	Is this a WebView / embedded software client
Is Mobile (is_mobile)	Is this a mobile device (e.g. a phone or tablet)

NeutrinoAPI/Bad Word Filter method

Parse, validate and get detailed user-agent information from a user agent string or from client hints.



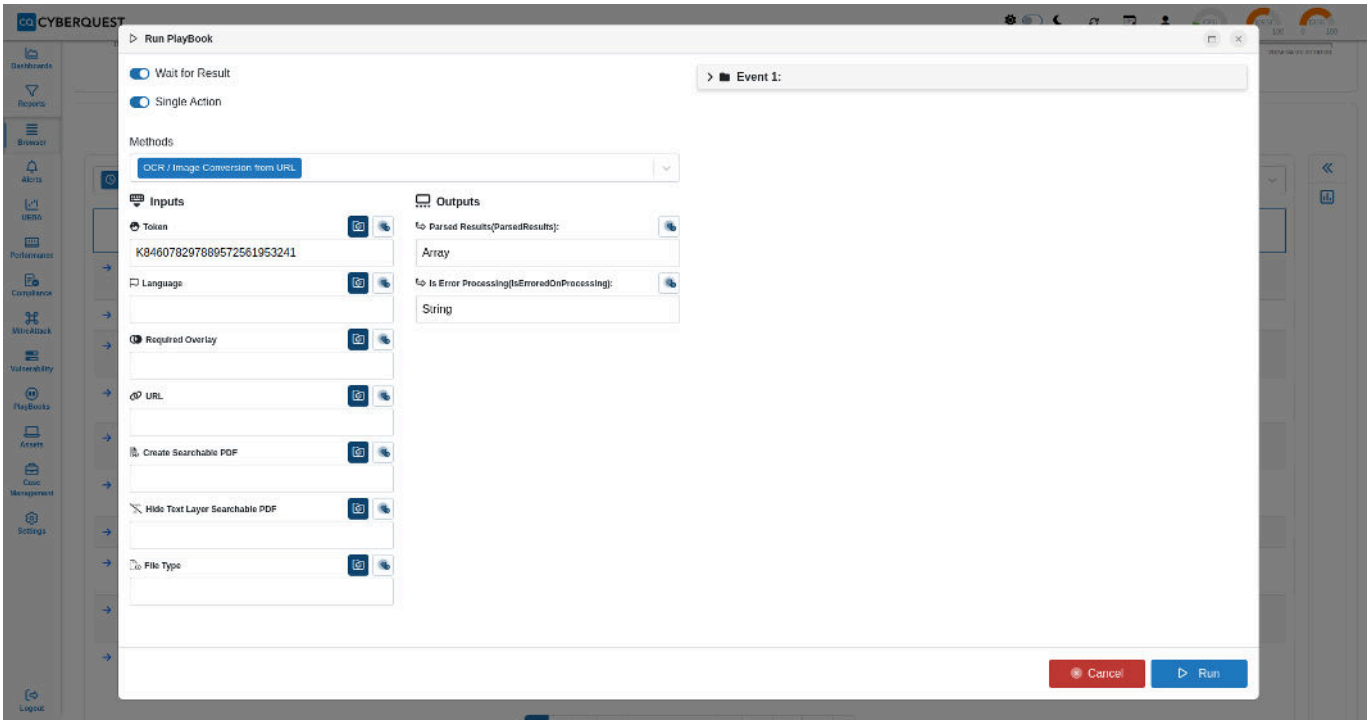
Inputs	Description
API Key (is required)	To use this API you must have an API Key from Neutrino Website
Username (is required)	The username used to Login on Neutrino Website
Content (is required)	The content to scan. This can be either a URL to load from, a file upload (multipart/form-data) or an HTML content string
Censor Character	The character to use to censor out the bad words found
Catalog	hich catalog of bad words to use, we currently maintain two bad word catalogs:strict - the largest database of bad words which includes profanity, obscenity, sexual, rude, cuss, dirty, swear and objectionable words and phrases. This catalog is suitable for environments of all ages including educational or childrens contentobscene - like the strict catalog but does not include any mild profanities, idiomatic phrases or words which are considered formal terminology. This catalog is suitable for adult environments where certain types of bad words are considered OK

Outputs	Description
Censored Content (censored_content)	The censored content (only set if censor-character has been set)
Bad Words Total (bad_words_total)	Total number of bad words detected
Bad Words List (bad_words_list)	An array of the bad words found

OCR

OCR/Image Conversion from URL method

Convert a image from an URL.

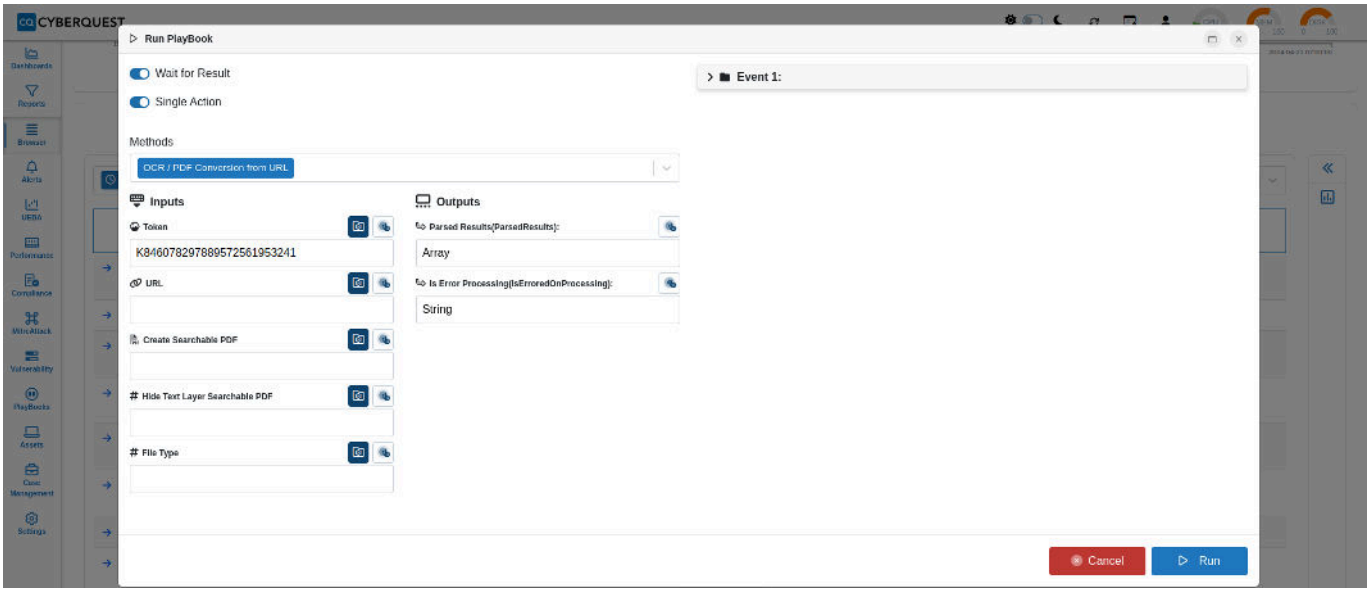


Inputs	Description
Token (is required)	To use the OCR API, you must have an API key
Language	Language used for OCR
Required Overlay	If true, returns the coordinates of the bounding boxes for each word. If false, the OCRed text is returned only as a text block (this makes the JSON reponse smaller). Overlay data can be used, for example, to show text over the image
URL	The URL from where it is retrieved the image
Create Searchable PDF	Default = FalseIf true, API generates a searchable PDF. This parameter automatically sets isOverlayRequired = true
Hide Text Layer Searchable PDF	Default = False. If true, the text layer is hidden (not visible)
File Type	Overwrites the automatic file type detection based on content-type. Supported image file formats are png, jpg (jpeg), gif, tif (tiff) and bmp. For document ocr, the api supports the Adobe PDF format. Multi-page TIFF files are supported

Outputs	Description
Parsed Results (ParsedResults)	The OCR results for the image or for each page of PDF. For PDF: Each page has its own OCR result and error message (if any)
Is Error Processing (IsErroredOnProcessing)	True if the API call was successful, otherwise false

OCR/PDF Conversion from URL method

Convert a PDF from a URL.

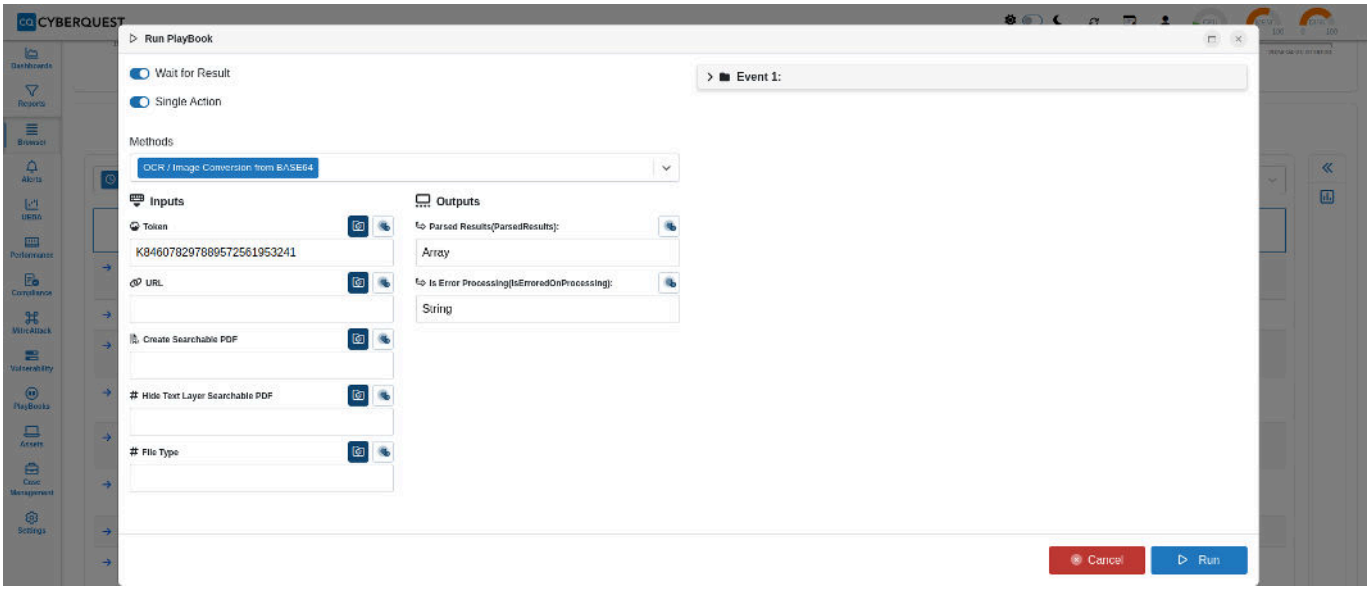


Inputs	Description
Token (is required)	To use the OCR API, you must have an API key.
URL	The URL from where it is converted the pdf
Create Searchable PDF	Default = FalseIf true, API generates a searchable PDF. This parameter automatically sets isOverlayRequired = true.
Hide Text Layer Searchable PDF	Default = False. If true, the text layer is hidden (not visible)
File Type	Overwrites the automatic file type detection based on content-type. Supported image file formats are png, jpg (jpeg), gif, tif (tiff) and bmp. For document ocr, the api supports the Adobe PDF format. Multi-page TIFF files are supported.

Outputs	Description
Parsed Results (ParsedResults)	The OCR results for the image or for each page of PDF. For PDF: Each page has its own OCR result and error message (if any)
Is Error Processing (IsErroredOnProcessing)	True if the API call was successful, otherwise false

OCR/Image Conversion from BASE64 method

Convert a image from an BASE64 String.

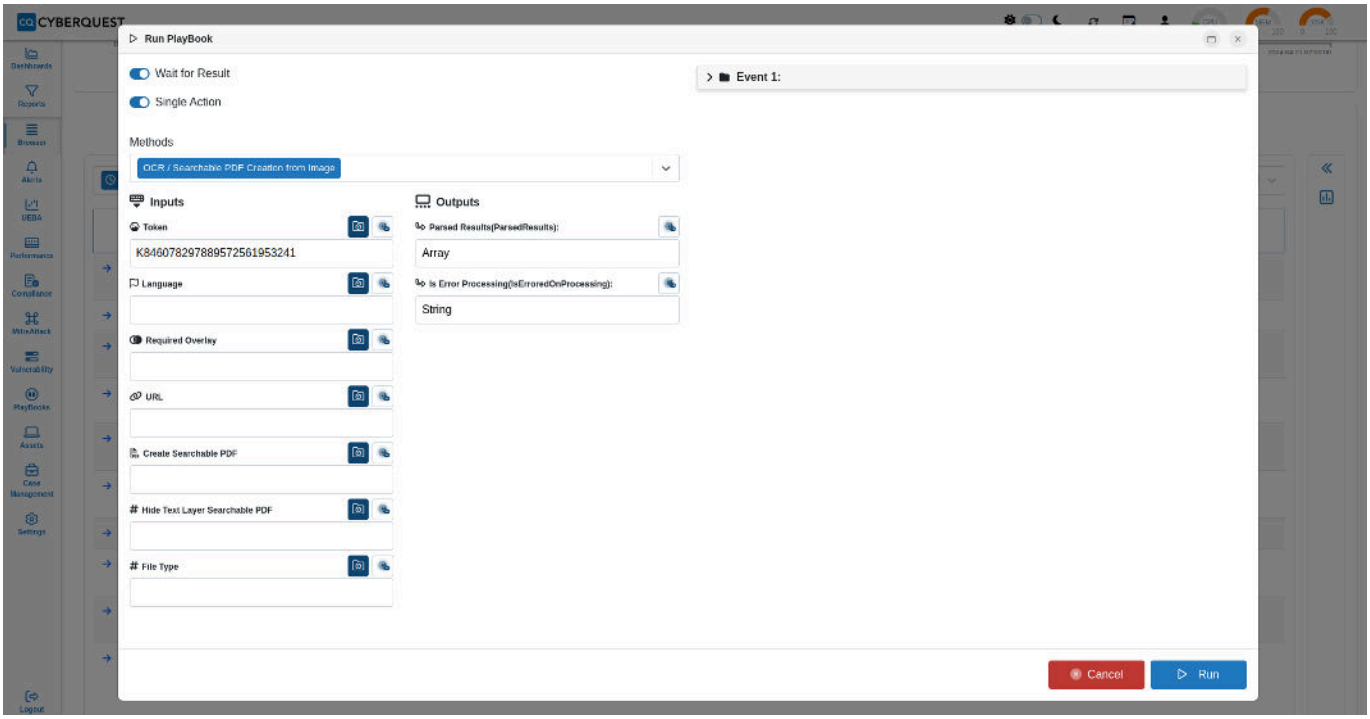


Inputs	Description
Token (is required)	To use the OCR API, you must have an API key.
URL	The BASE64 string from where it is converted the image
Create Searchable PDF	Default = FalseIf true, API generates a searchable PDF. This parameter automatically sets isOverlayRequired = true.
Hide Text Layer Searchable PDF	Default = False. If true, the text layer is hidden (not visible)
File Type	Overwrites the automatic file type detection based on content-type. Supported image file formats are png, jpg (jpeg), gif, tif (tiff) and bmp. For document ocr, the api supports the Adobe PDF format. Multi-page TIFF files are supported.

Outputs	Description
Parsed Results (ParsedResults)	The OCR results for the image or for each page of PDF. For PDF: Each page has its own OCR result and error message (if any)
Is Error Processing (IsErroredOnProcessing)	True if the API call was successful, otherwise false

OCR/Searchable PDF Creation from Image method

Create Searchable PDF from image.



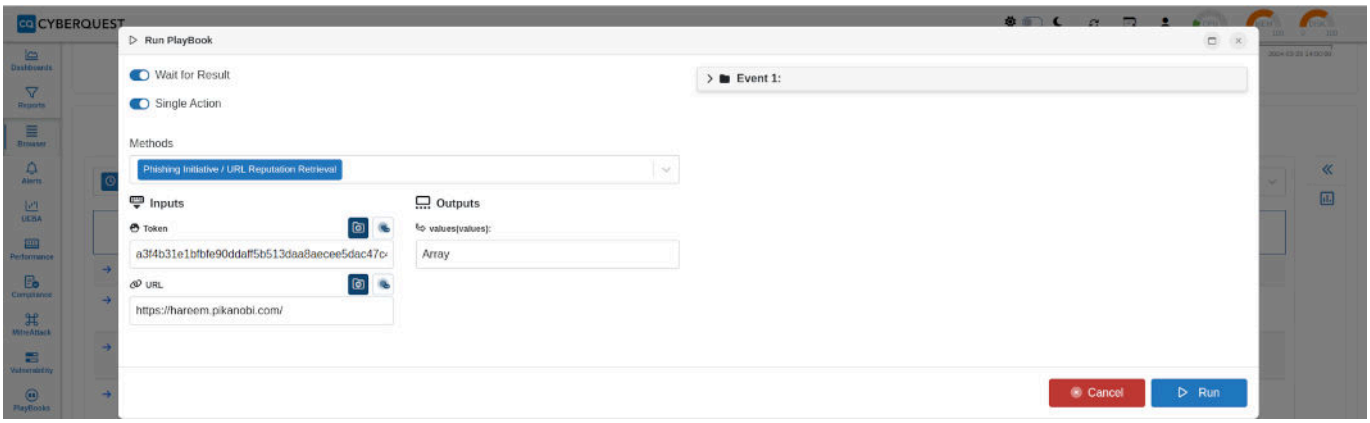
Inputs	Description
Token (is required)	To use the OCR API, you must have an API key
Language	Language used for OCR
Required Overlay	If true, returns the coordinates of the bounding boxes for each word. If false, the OCRed text is returned only as a text block (this makes the JSON reponse smaller). Overlay data can be used, for example, to show text over the image
URL	The image from where it is created Searchable PDF
Create Searchable PDF	Default = FalseIf true, API generates a searchable PDF. This parameter automatically sets isOverlayRequired = true
Hide Text Layer Searchable PDF	Default = False. If true, the text layer is hidden (not visible)
File Type	Overwrites the automatic file type detection based on content-type. Supported image file formats are png, jpg (jpeg), gif, tif (tiff) and bmp. For document ocr, the api supports the Adobe PDF format. Multi-page TIFF files are supported.

Outputs	Description
Parsed Results (ParsedResults)	The OCR results for the image or for each page of PDF. For PDF: Each page has its own OCR result and error message (if any)
Is Error Processing (IsErroredOnProcessing)	True if the API call was successful, otherwise false

Phishing Initiative

Phishing Initiative/URL Reputation Retrieval method

Retrieving the reputation of a URL that you have specified.



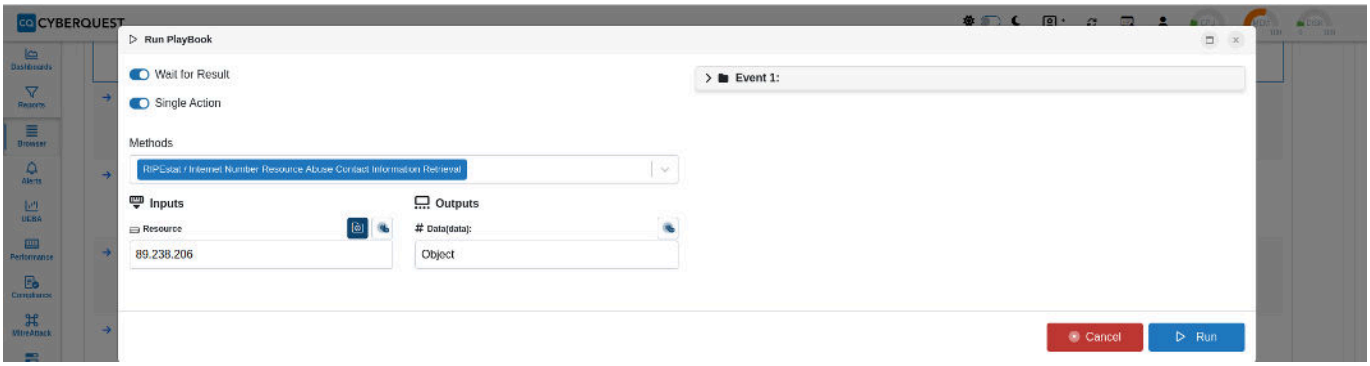
Inputs	Description
Token (is required)	To use the PhishingInitiative API, you must have an API key.
URL (is required)	The URL that is being searched

Outputs	Description
values (values)	The results of the API call

RIPEstat

RIPEstat/Internet Number Resource Abuse Contact Information Retrieval method

This data calls primary goal is to return abuse contact information for an Internet number resource.

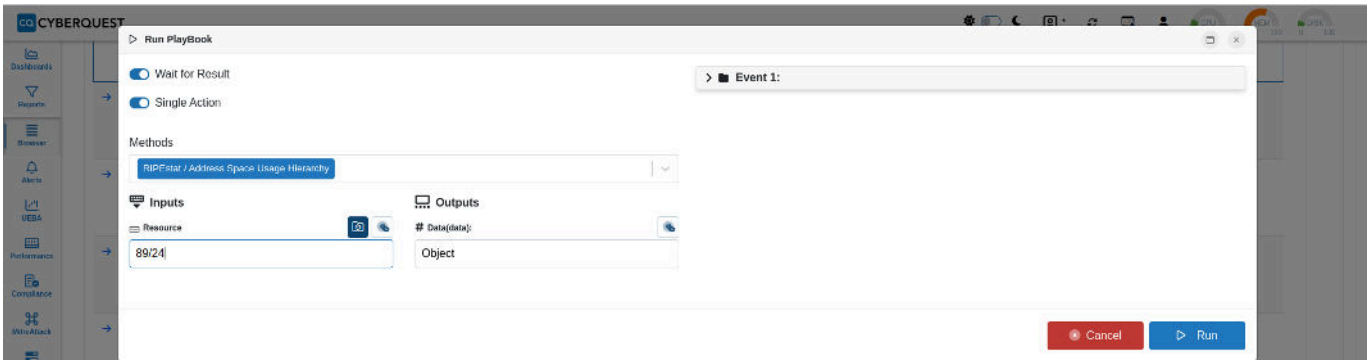


Inputs	Description
Resource (is required)	This is the resource the query is based on.

Outputs	Description
Data (data)	The results of the API call

RIPEstat/Address Space Usage Hierarchy method

This data call returns address space objects (inetnum or inet6num) from the RIPE Database related to the queried resource.

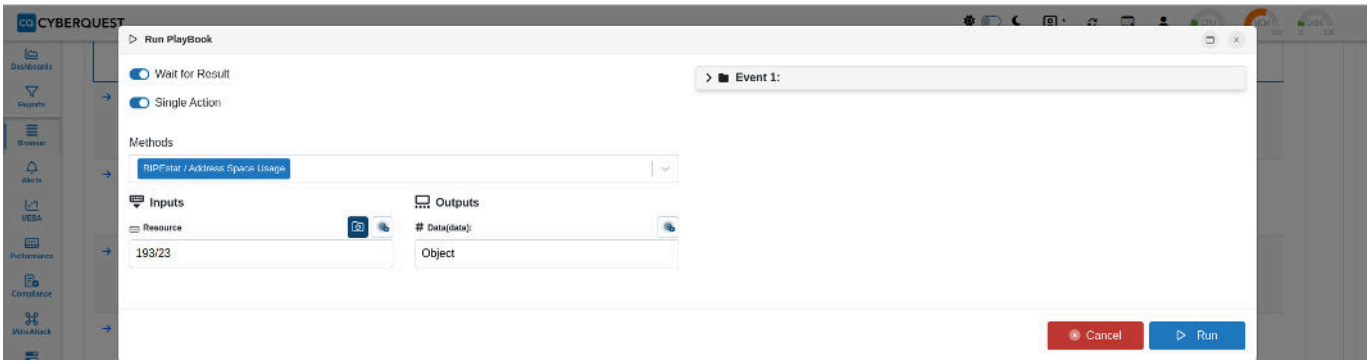


Inputs	Description
Resource (is required)	The prefix or IP range the address space hierarchy should be returned for.

Outputs	Description
Data (data)	The results of the API call

RIPEstat/Address Space Usage method

This data call displays the usage of a prefix or IP range based on the objects currently in the RIPE database.

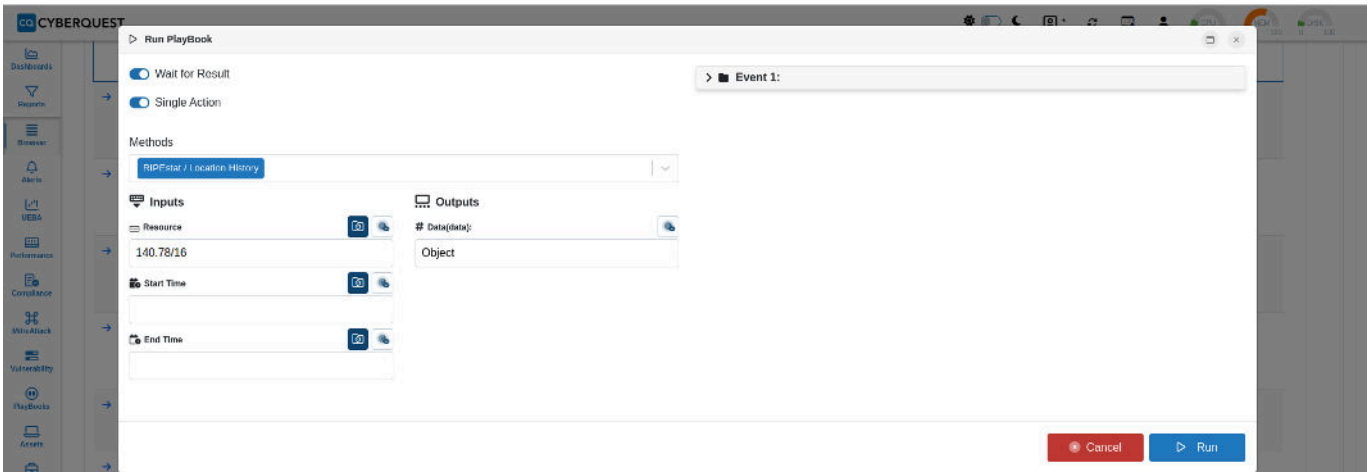


Inputs	Description
Resource (is required)	States the prefix or IP range the address space usage should be returned for

Outputs	Description
Data (data)	The results of the API call

RIPEstat/Location History method

This data call returns information supplied by IANA and RIRs for allocations and direct assignments of prefixes and AS numbers of time.

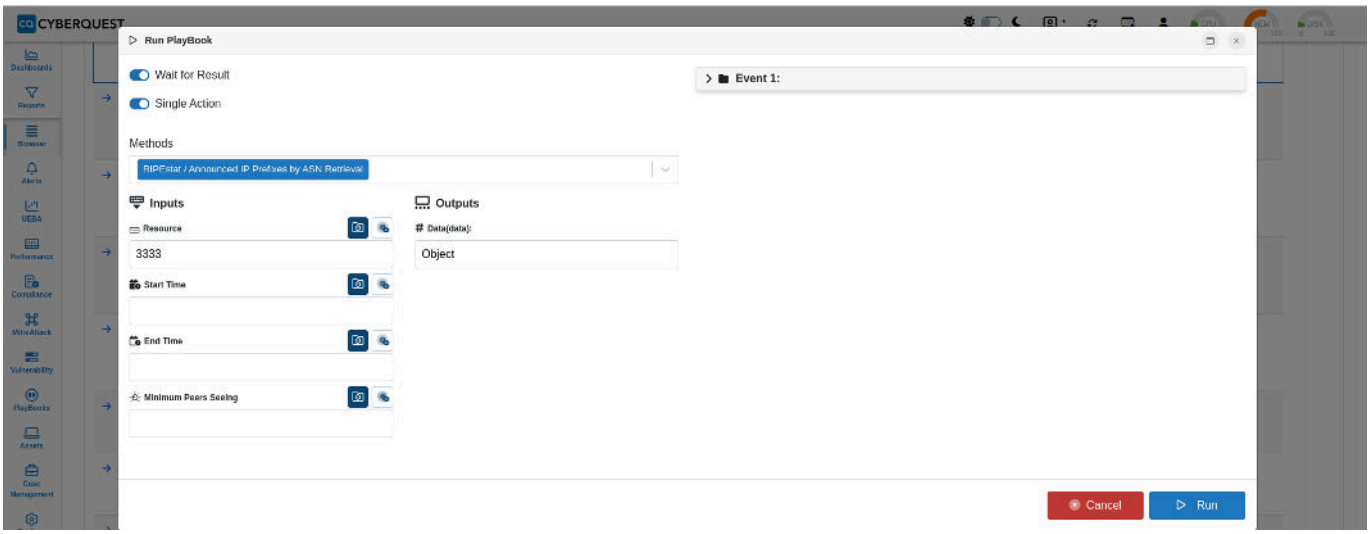


Inputs	Description
Resource (is required)	This is the resource the query is based on.
Start Time	Defines the starttime for the query
End Time	Defines the endtime for the query

Outputs	Description
Data (data)	The results of the API call

RIPEstat/Announced IP Prefixes by ASN Retrieval method

This API request provides a list of announced IP prefixes associated with a given ASN. The results can be filtered based on a specific time frame if desired.

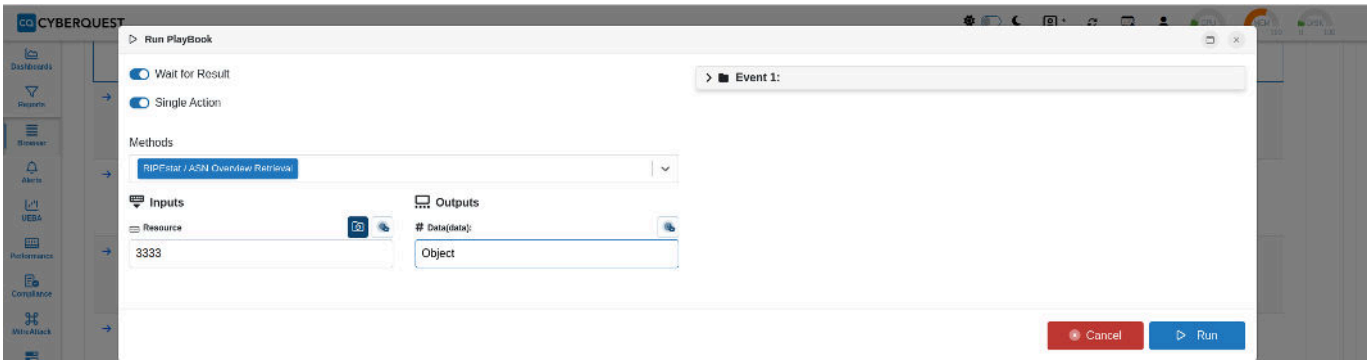


Inputs	Description
Resource (is required)	The Autonomous System Number for which to return prefixes.
Start Time	The start time for the query.
End Time	The end time for the query.
Minimum Peers Seeing	Minimum number of RIS peers seeing the prefix for it to be included in the results. Excludes low-visibility/localized announcements

Outputs	Description
Data (data)	The results of the API call

RIPEstat/ASN Overview Retrieval method

This data call provides an overview of an ASN, including its announcement status and the name of its holder based on the WHOIS service.

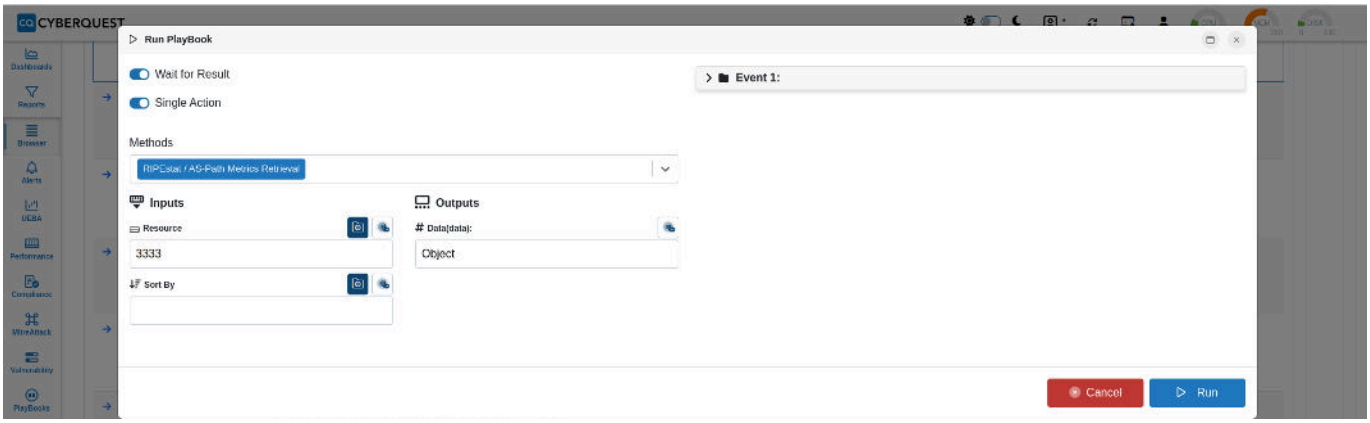


Inputs	Description
Resource (is required)	States the as you want to get the resource info for

Outputs	Description
Data (data)	The results of the API call

RIPEstat/AS-Path Metrics Retrieval method

This data call retrieves AS-path metrics for the queried ASN, such as the shortest or longest AS-path to other ASNs that we are peering with.

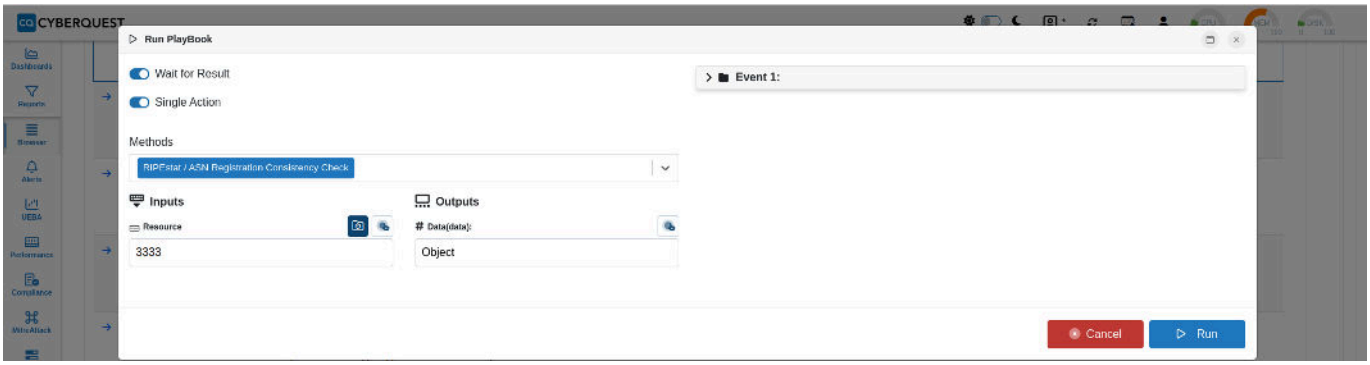


Inputs	Description
Resource (is required)	AS number to query
Sort By	Sort by the given field. In the case of geo, sort by approximating a world map on to a circle.

Outputs	Description
Data (data)	The results of the API call

RIPEstat/ASN Registration Consistency Check method

This data call examines the consistency between the registration information for an ASN in the internet routing registry (IRR) and what is observed in RIS BGP tables.

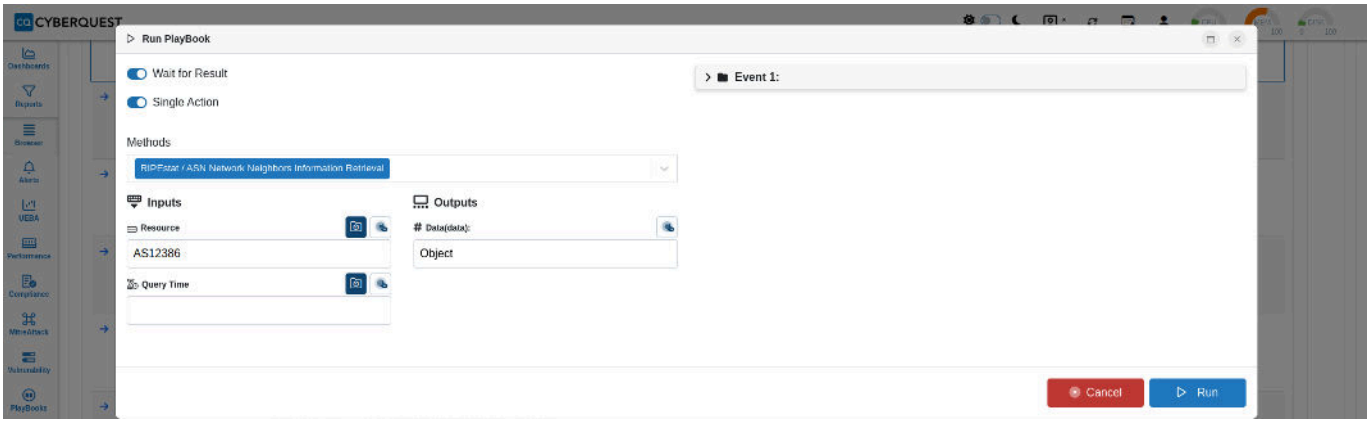


Inputs	Description
Resource (is required)	The ASN to query

Outputs	Description
Data (data)	The results of the API call

RIPEstat/ASN Network Neighbors Information Retrieval method

This data call provides information on the network neighbors for a given ASN as observed in RIS. It includes statistical information and the list of observed ASN neighbors.

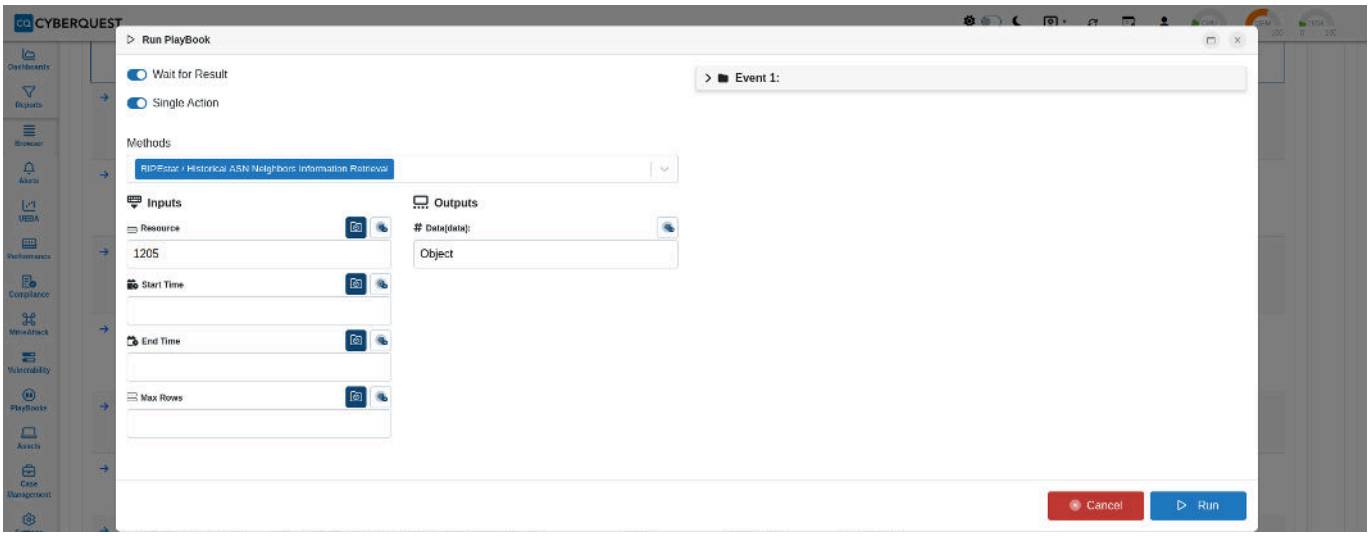


Inputs	Description
Resource (is required)	The data call will return all neighbours found for this ASN.
Query Time	Defines the query time for the query.If not set, the start time will be set to the latest available data point.

Outputs	Description
Data (data)	The results of the API call

RIPEstat/Historical ASN Neighbors Information Retrieval method

This data call provides information about the neighboring ASNs of a queried ASN, extended with historical data. It includes details about the ASNs that have been observed as neighbors over time.

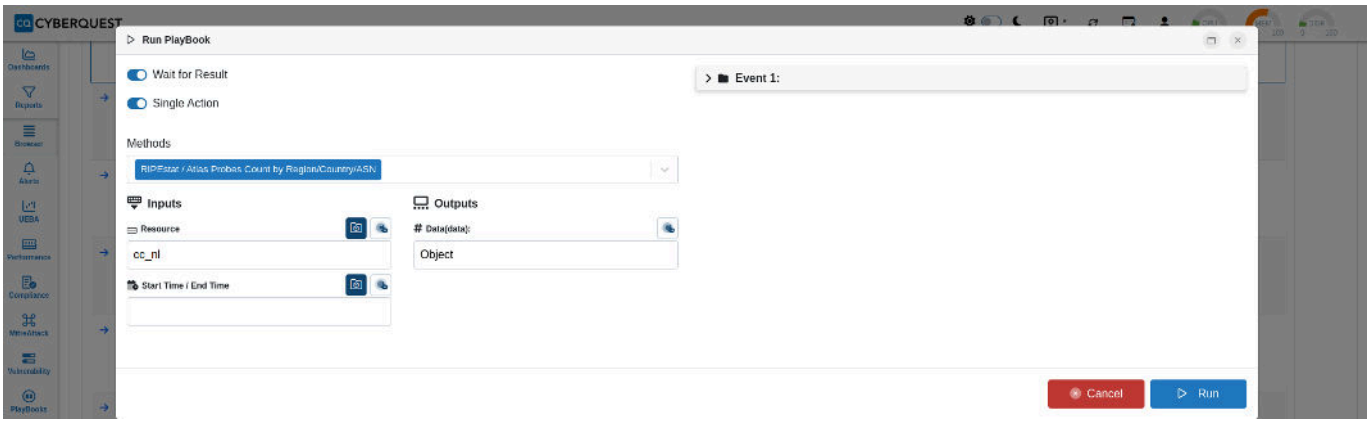


Inputs	Description
Resource (is required)	This is the ASN the neighbours are shown for.
Start Time	Defines the query starttime for the query
End Time	Defines the query endtime for the query
Max Rows	Defines the limit of neighbours to be included in the result, e.g. max_rows=50 means the result will be truncated to 50 neighbours. Has not effect if there are less neighbours anyway.

Outputs	Description
Data (data)	The results of the API call

RIPEstat/Atlas Probes Count by Region/Country/ASN method

This data call provides information on the number of RIPE Atlas probes in a region, a country or network (ASN).

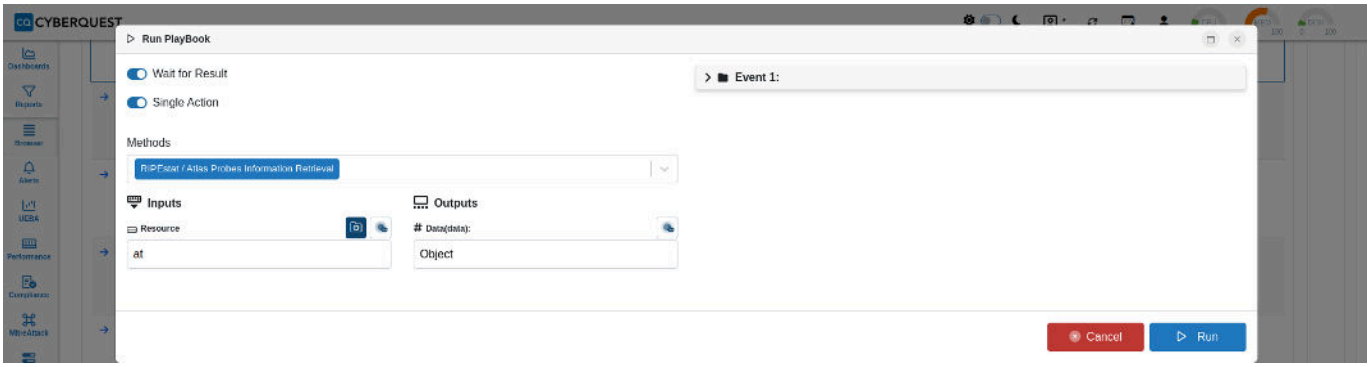


Inputs	Description
Resource (is required)	Due to the ambigious nature of abbreviated identifiers for regions and countries (e.g. me for Middle East and Montenegro) region and country resources should be prefixes with region_ or cc_.Looking up a network can be specified on the IP version by using the prefix asn4_ for IP v4 networks and asn6_ for IP v6 networks.For mixed results the resources just need to be comma separated
Start Time / End Time	Can be used to set the time range of the lookup and the output.

Outputs	Description
Data (data)	The results of the API call

RIPEstat/Atlas Probes Information Retrieval method

This data call returns information on RIPE Atlas probes in an ASN, a prefix, or a country.

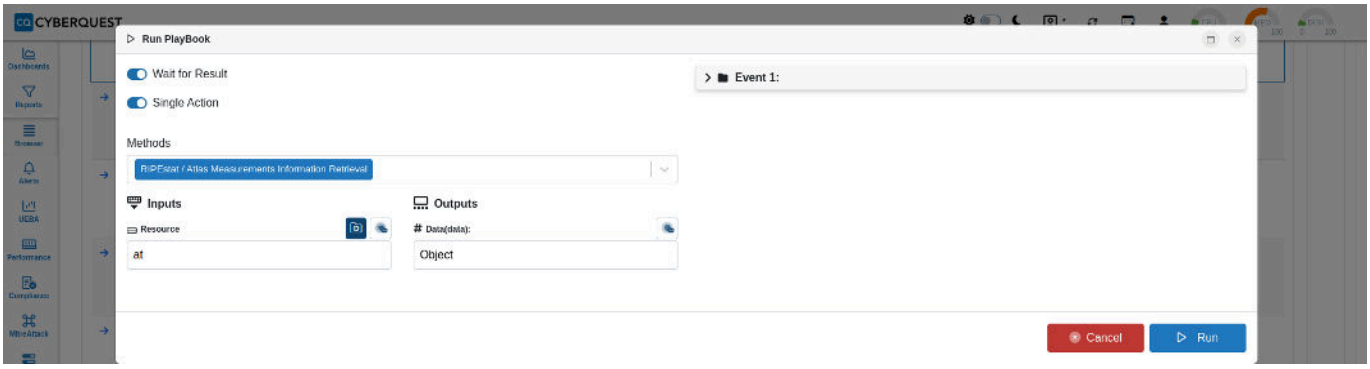


Inputs	Description
Resource (is required)	Prefix, network (ASN) or country

Outputs	Description
Data (data)	The results of the API call

RIPEstat/Atlas Measurements Information Retrieval method

This data call provides information on the RIPE Atlas measurements that target an network (ASN), a prefix or a hostname.

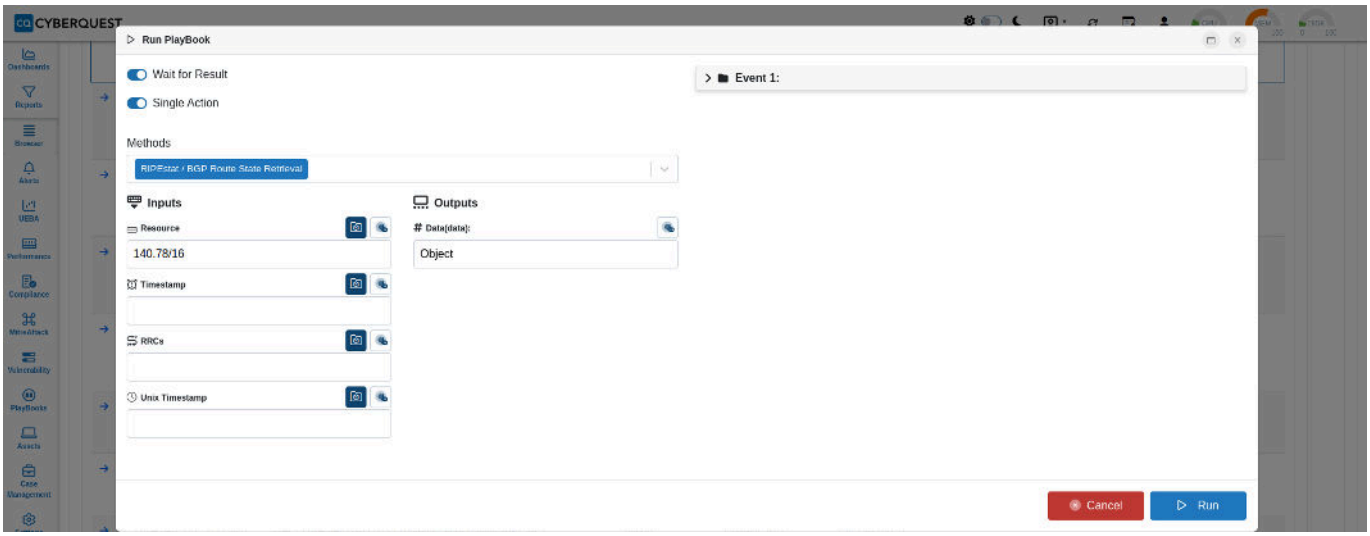


Inputs	Description
Resource (is required)	Prefix, network (ASN) or hostname

Outputs	Description
Data (data)	The results of the API call

RIPEstat/BGP Route State Retrieval method

This data call delivers the state of BGP routes for a resource as observed by all RIS collectors at a given point in time.

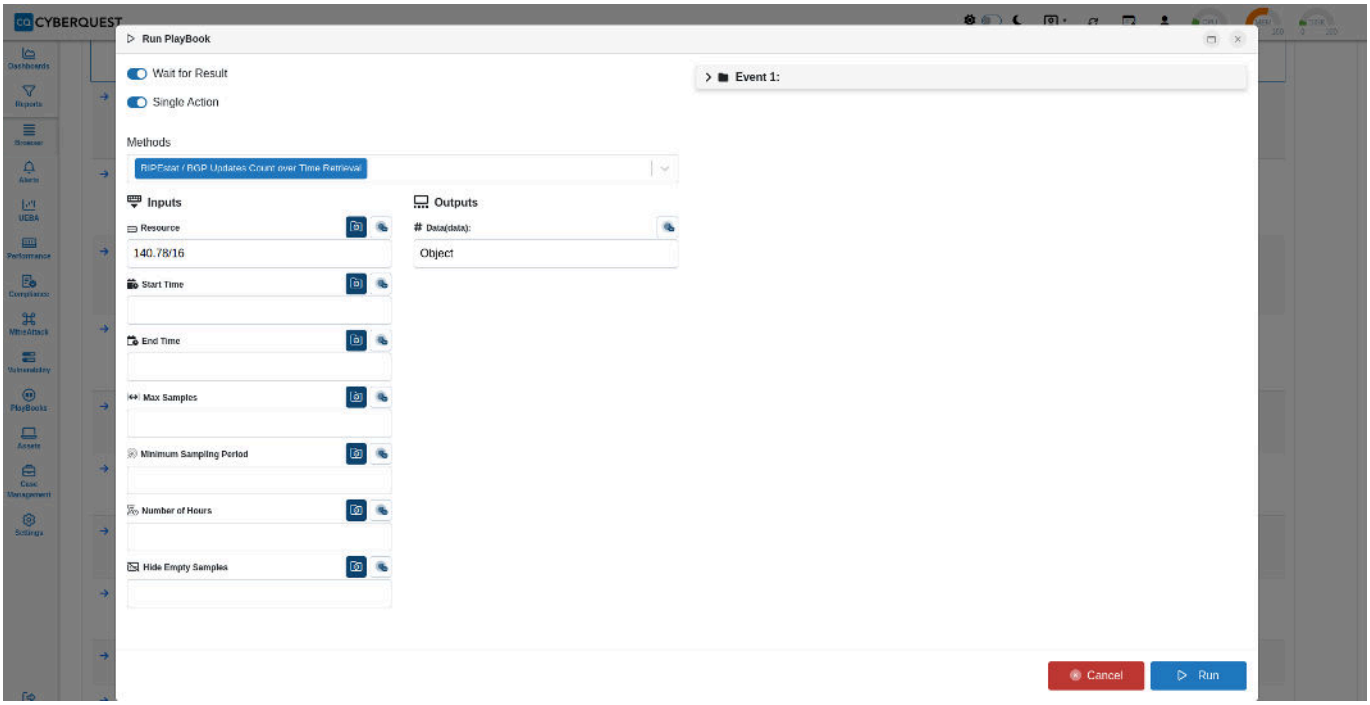


Inputs	Description
Resource (is required)	Defines the resource that the query is performed for. If a list of resources is supplied, the results will be combined for all of them
Timestamp	Defines the time for when to perform the query
RRCs	The list of Route Collectors (RRCs) to get the results from
Unix Timestamp	If TRUE, will format the timestamps in the result as Unix timestamp

Outputs	Description
Data (data)	The results of the API call

RIPEstat/BGP Updates Count over Time Retrieval method

The number of BGP updates seen over time is returned by this data request. The aggregated results are shown in time intervals whose length is determined by the input parameters.

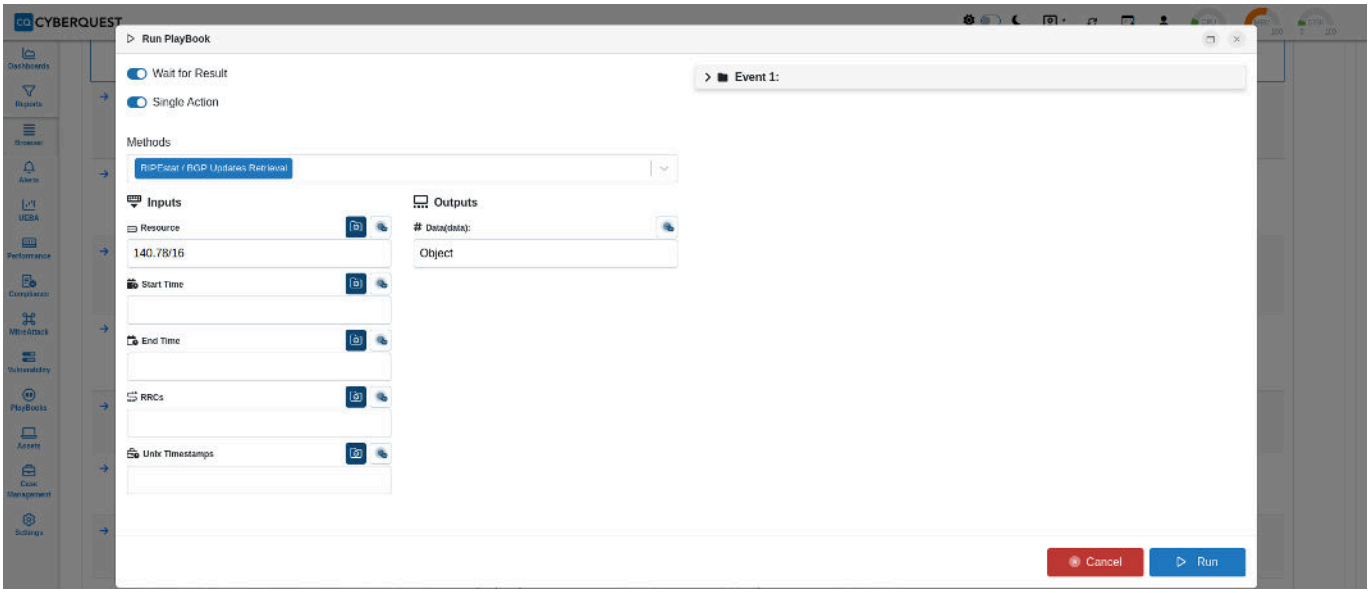


Inputs	Description
Resource (is required)	Defines the resource the query is carried out on
Start Time	Defines the starttime for the query
End Time	Defines the endtime for the query
Max Samples	BGP events are aggregated in to at most this number of sampling periods
Minimum Sampling Period	The smallest possible time period for each interval. It will be automatically increased to satisfy max_samples
Number of Hours	Number of hours to look back. If no starttime and endtime are provided this parameter will be used to calculate starttime from the deafult endtime (which is now).
Hide Empty Samples	If true (default) then samples with 0 updates will not be returned - they are simply implied by the returned query_startendtime/query_endtime.

Outputs	Description
Data (data)	The results of the API call

RIPEstat/BGP Updates Retrieval method

This data call returns the BGP updates for a resource over a specified time period.

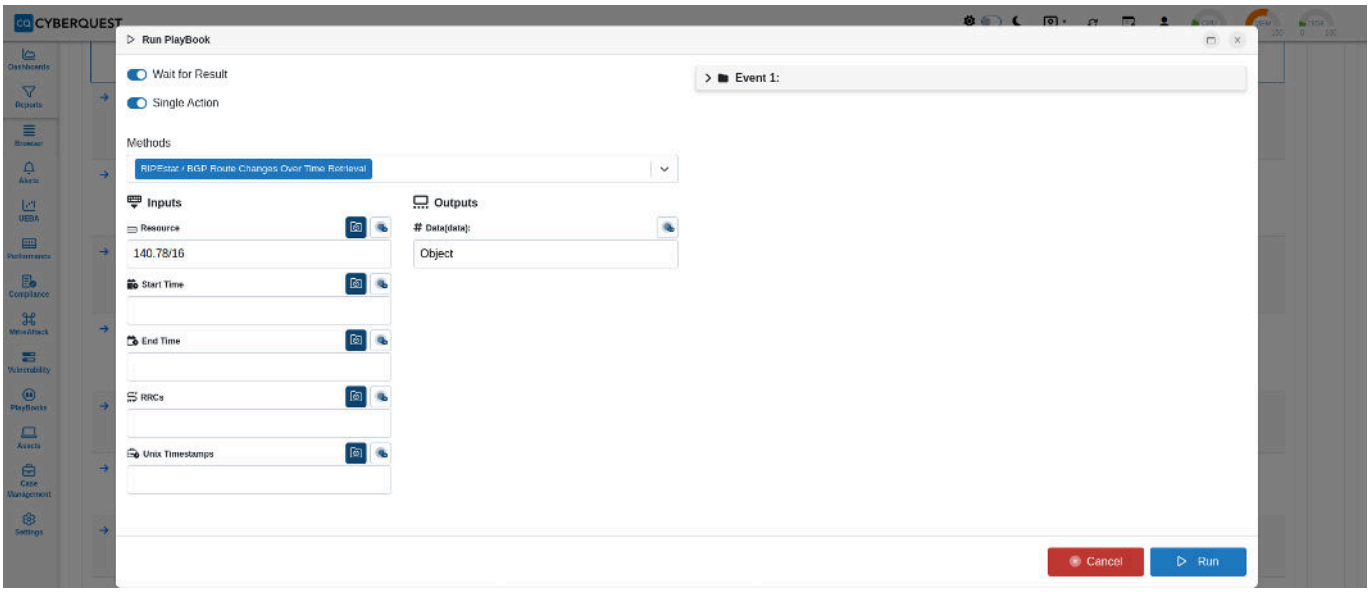


Inputs	Description
Resource (is required)	Defines the resource that the query is performed for. If a list of resources is supplied, the results will be combined for all of them.
Start Time	Defines the starttime for the query
End Time	Defines the endtime for the query
RRCs	The list of Route Collectors (RRCs) to get the results from
Unix Timestamps	If TRUE, will format the timestamps in the result as Unix timestamp.

Outputs	Description
Data (data)	The results of the API call

RIPEstat/BGP Route Changes Over Time Retrieval method

This data call represents the scenario of what occurred to the BGP routes of a resource over a period of time.

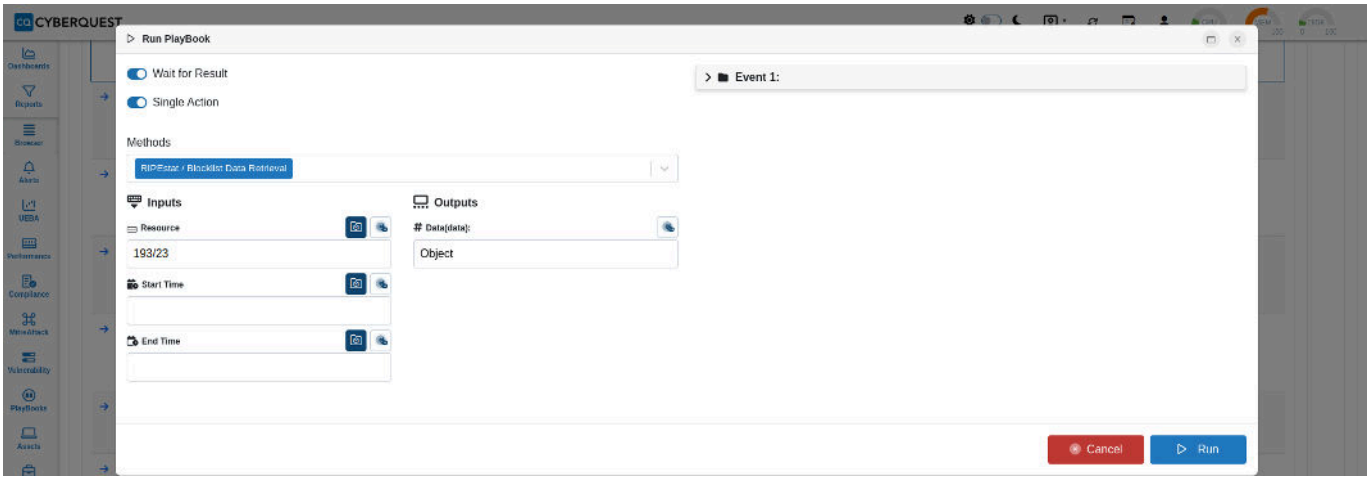


Inputs	Description
Resource (is required)	Defines the resource that the query is performed for. If a list of resources is supplied, the results will be combined for all of them.
Start Time	Defines the starttime for the query
End Time	Defines the endtime for the query
RRCs	The list of Route Collectors (RRCs) to get the results from.
Unix Timestamps	If TRUE, will format the timestamps in the result as Unix timestamp.

Outputs	Description
Data (data)	The results of the API call

RIPEstat/Blocklist Data Retrieval method

This data call returns blocklist related data for a queried resource.

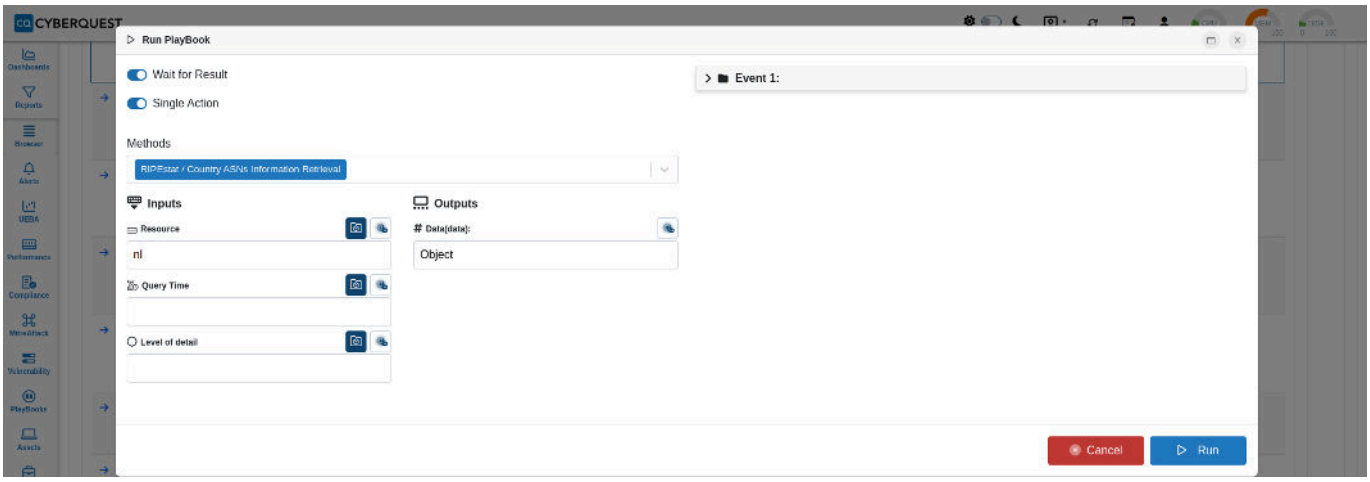


Inputs	Description
Resource (is required)	States the prefix or IP range you want to get blocklist information for
Start Time	Defines the starttime for the query
End Time	Defines the endtime for the query

Outputs	Description
Data (data)	The results of the API call

RIPEstat/Country ASNs Information Retrieval method

This data call returns information on the registered and routed ASNs of a country.



Inputs	Description
Resource (is required)	The country has to be provided as an ISO-3166-1 alpha-2 country code.
Query Time	Defines the time of the lookup. This value needs to be or will be aligned to the RIS dump times!
Level of detail	Defines the level of detail in which the data is being returned.Levels are:* 0 - Least detailed output* 1 - Most detailed output

Outputs	Description
Data (data)	The results of the API call

RIPEstat/Country Internet Resources Information Retrieval method

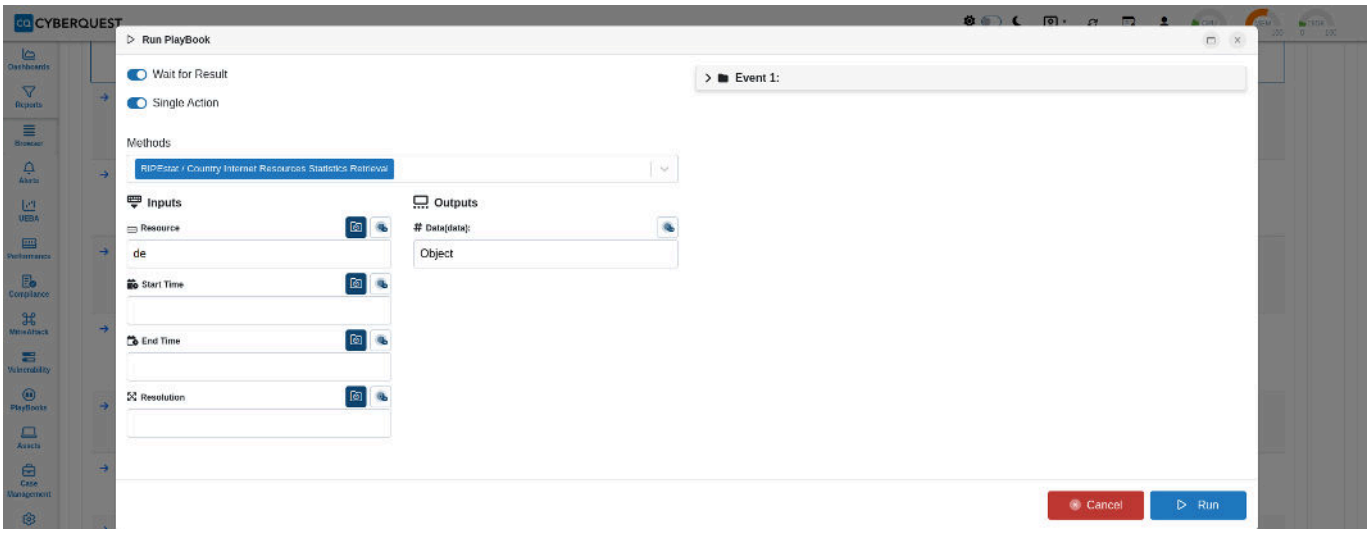
This data call returns information about the Internet resources associated with a country, such as ASNs, IPv4 ranges, and IPv4/6 CIDR prefixes.

Inputs	Description
Resource (is required)	The country to find IP prefixes and AS numbers for.
Time	The time to query. By default, returns the latest available data. This value is truncated to midnight
IPv4 Format	Describes the formatting for the output of IPv4 space.

Outputs	Description
Data (data)	The results of the API call

RIPEstat/Country Internet Resources Statistics Retrieval method

This data call returns statistics on Internet resources for a country, this includes:number of ASNs seen in routing data and registration data;number of prefixes in routing data and registration data (split into IPv4 and IPv6);amount of IPv4 space seen in routing data as well as registration data.

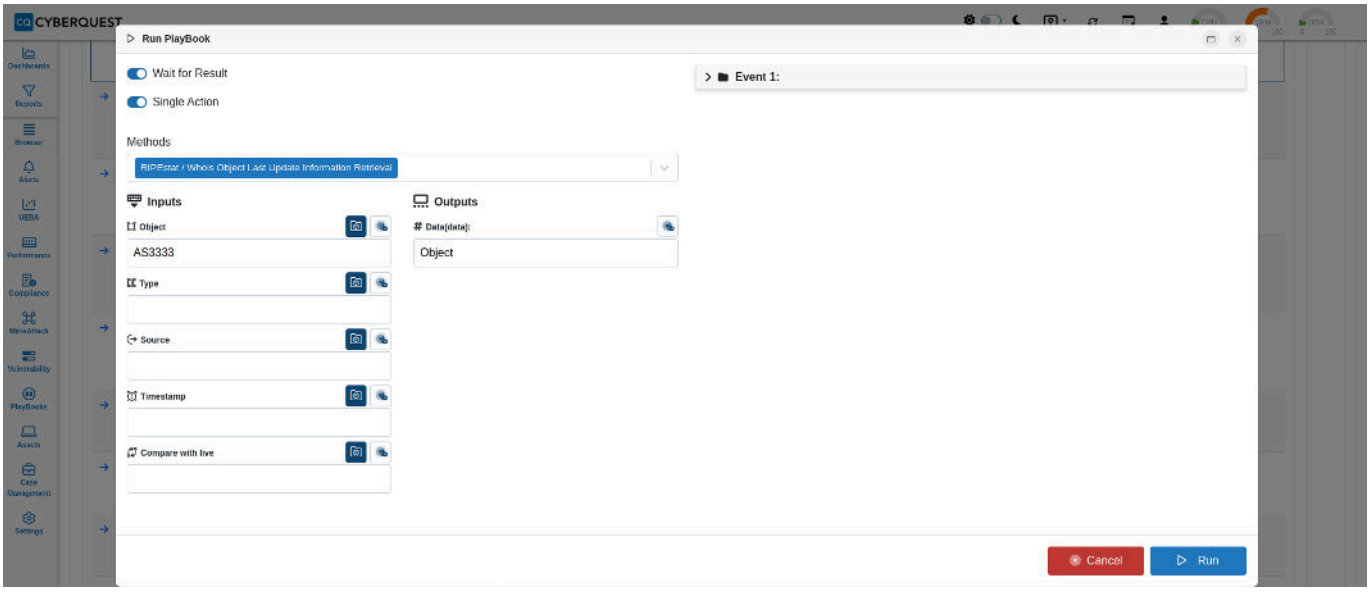


Inputs	Description
Resource (is required)	This is the resource the query is based on.
Start Time	Defines the country that the stats are returned for
End Time	The end time for the query. See Default Values for Time Parameters for details.
Resolution	Possible values:* 5m - 5 minutes* 1h - 1 hour* 1d - 1 day* 1w - 1 week

Outputs	Description
Data (data)	The results of the API call

RIPEstat/Whois Object Last Update Information Retrieval method

This data call returns information of when a certain object was last updated in the whois database.

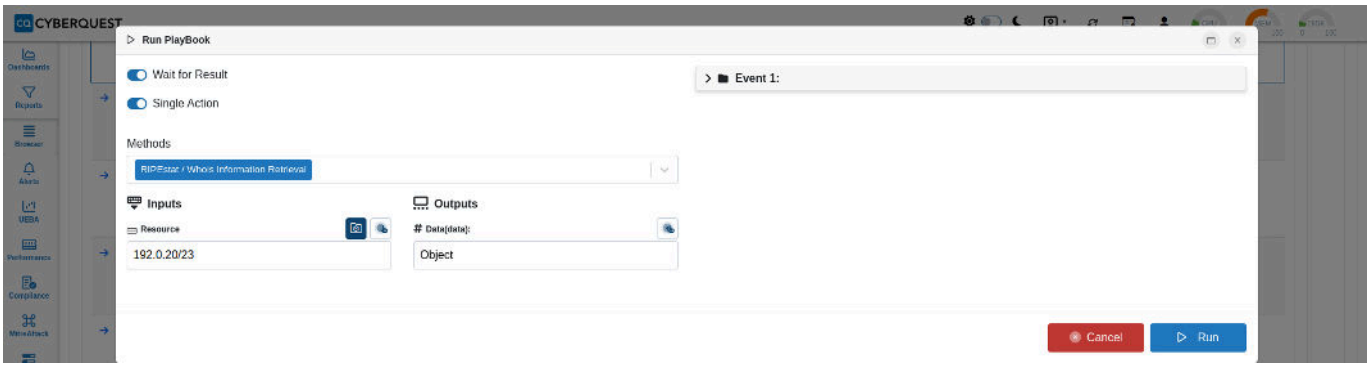


Inputs	Description
Object	The exact object to query for
Type	Examples: aut-num, inetnum, person, etc
Source	RIPE or APNIC
Timestamp	Defines the time for which to perform the query
Compare with live	When True (default), the version at the last changed time will be compared with the current live object and indicate if its different. This will indicate whether there has been at least one modification between query_time and now.

Outputs	Description
Data (data)	The results of the API call

RIPEstat/Whois Information Retrieval method

This data call returns whois information from the relevant Regional Internet Registry and Routing Registry.

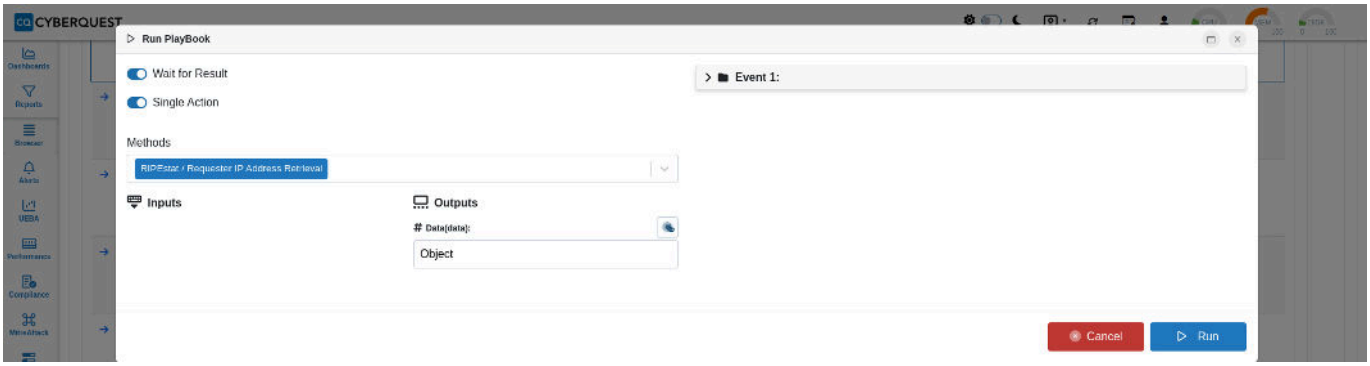


Inputs	Description
Resource (is required)	ASN/IPv4/IPv6/IP Range

Outputs	Description
Data (data)	The results of the API call

RIPEstat/Requester IP Address Retrieval method

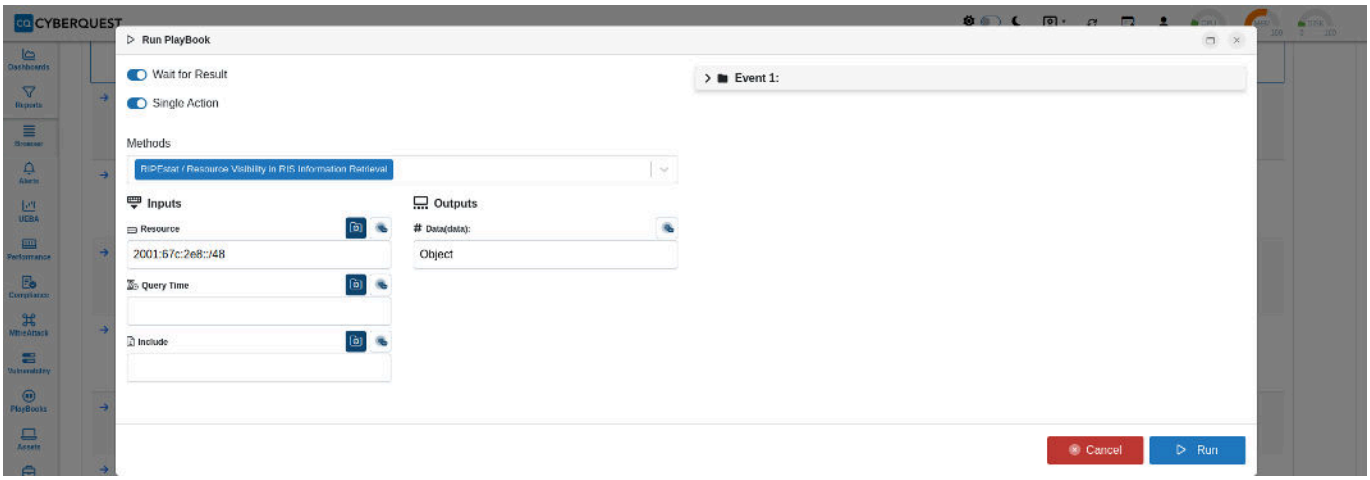
This data call returns the IP address of the requester.



Outputs	Description
Data (data)	The results of the API call

RIPEstat/Resource Visibility in RIS Information Retrieval method

This data call provides information on the visibility of a resource as observed from RIS.

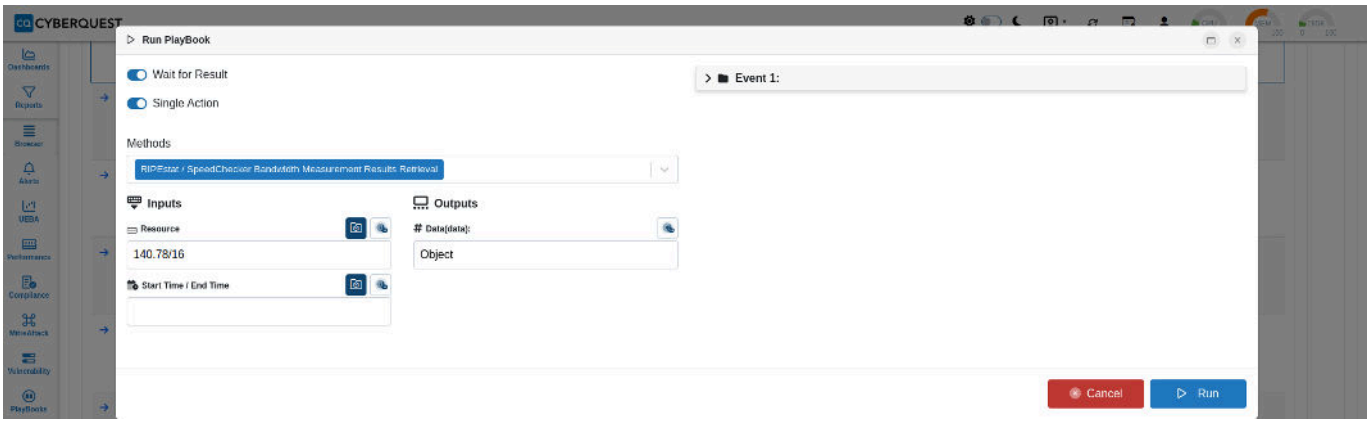


Inputs	Description
Resource (is required)	This is the resource the query is based on.
Query Time	Defines the time of the lookup. This value will be automatically aligned to a RIS colletion time.
Include	This parameter defines additional data to be included.peers_seeing includes details on peers that are seeing a resource as only the peers that are not seeing a resource. By default it is not set because the output become significantly bigger.

Outputs	Description
Data (data)	The results of the API call

RIPEstat/SpeedChecker Bandwidth Measurement Results Retrieval method

This data call provides bandwidth measurement results collected on the SpeedChecker platform.

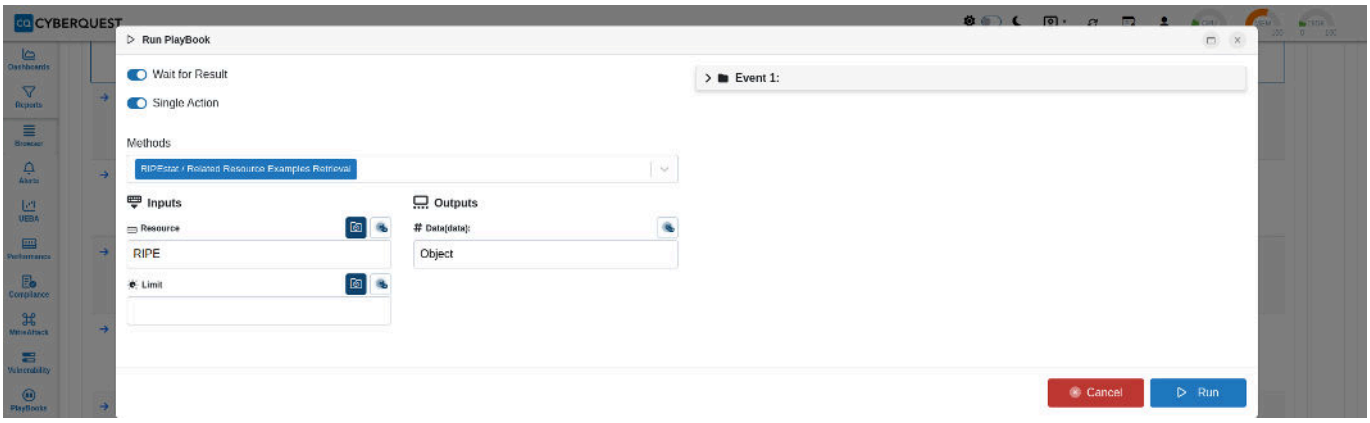


Inputs	Description
Resource (is required)	At this moment the data call only supports prefixes but aggregations for ASNs and countries is planned.
Start Time / End Time	The start/end time defining the upper and lower boundary of the lookup.

Outputs	Description
Data (data)	The results of the API call

RIPEstat/Related Resource Examples Retrieval method

This data call returns example resource that are directly or indirectly related to the given input.

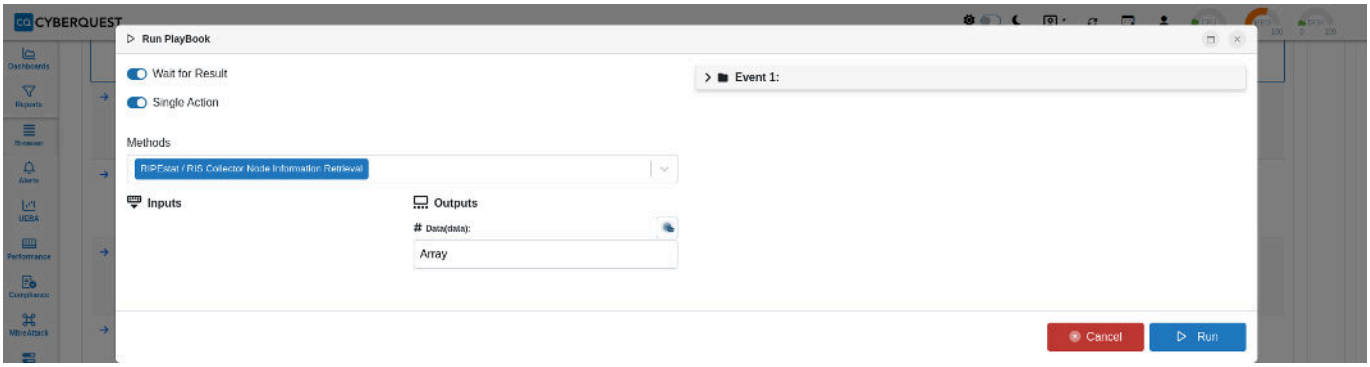


Inputs	Description
Resource (is required)	This is the resource the query is based on.
Limit	Defines how many suggestions are returned per category

Outputs	Description
Data (data)	The results of the API call

RIPEstat/RIS Collector Node Information Retrieval method

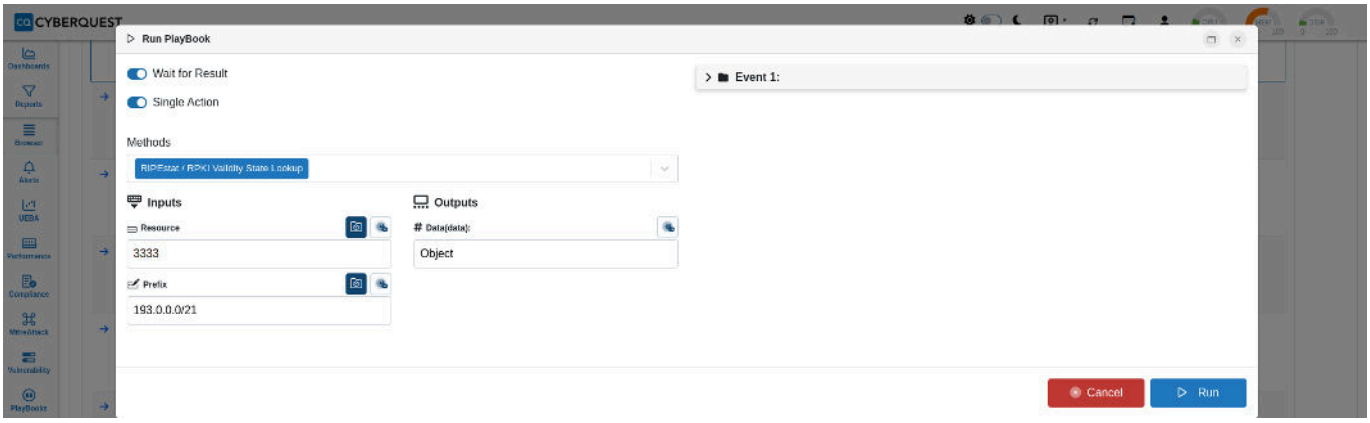
This data call provides (meta) information on collector nodes (RRCs) of the RIS network.



Outputs	Description
Data (data)	The results of the API call

RIPEstat/RPKI Validity State Lookup method

This data call returns the RPKI validity state for a combination of prefix and Autonomous System. This combination will be used to perform the lookup against the RPKI validator Routinator, and then return its RPKI validity state.

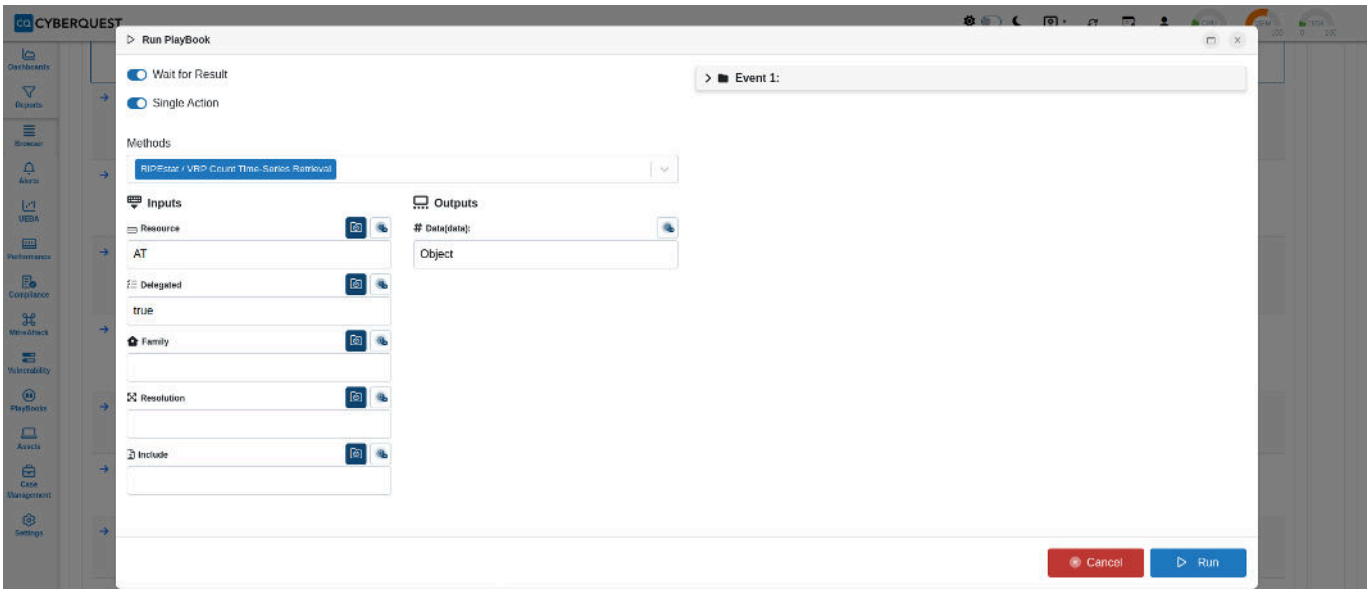


Inputs	Description
Resource (is required)	The ASN used to perform the RPKI validity state lookup.
Prefix (is required)	The prefix to perform the RPKI validity state lookup. Note the prefixs length is also taken from this field.

Outputs	Description
Data (data)	The results of the API call

RIPEstat/VRP Count Time-Series Retrieval method

This data call returns a time-series with the count of VRPs (Validated ROA Payload) for the requested resource.

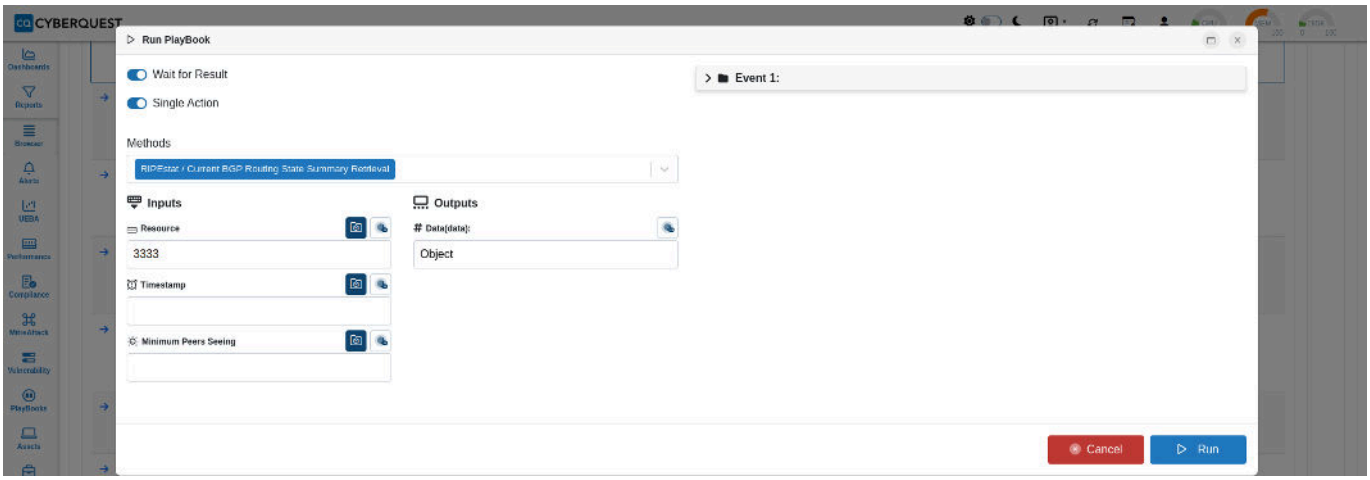


Inputs	Description
Resource (is required)	The resource to query for. The query returns only matches, for each case:Prefix: those VRPs which have an exact matching prefixASN: those VRPs which have a matching origin.Country code: those VRPs which are registered under a certain country (according to delegated files).Trust anchor: those VRPs which have ROAs under a certain trust anchor.
Delegated	If present, the response will include registration information for that resource.
Family	IP address family to filter for
Resolution	Time bin to group the result by. All values except d will return a response with min, avg, max, first, last, and samples.This option doesnt apply when using `include=ranges`.
Include	count: return the count of VRPs for the queried resource.ranges: the VRPs related to the queried resource, in the form of time ranges.

Outputs	Description
Data (data)	The results of the API call

RIPEstat/Current BGP Routing State Summary Retrieval method

This data call returns a summary of the current BGP routing state of a given IP prefix or ASN, as observed by the RIS route collectors.

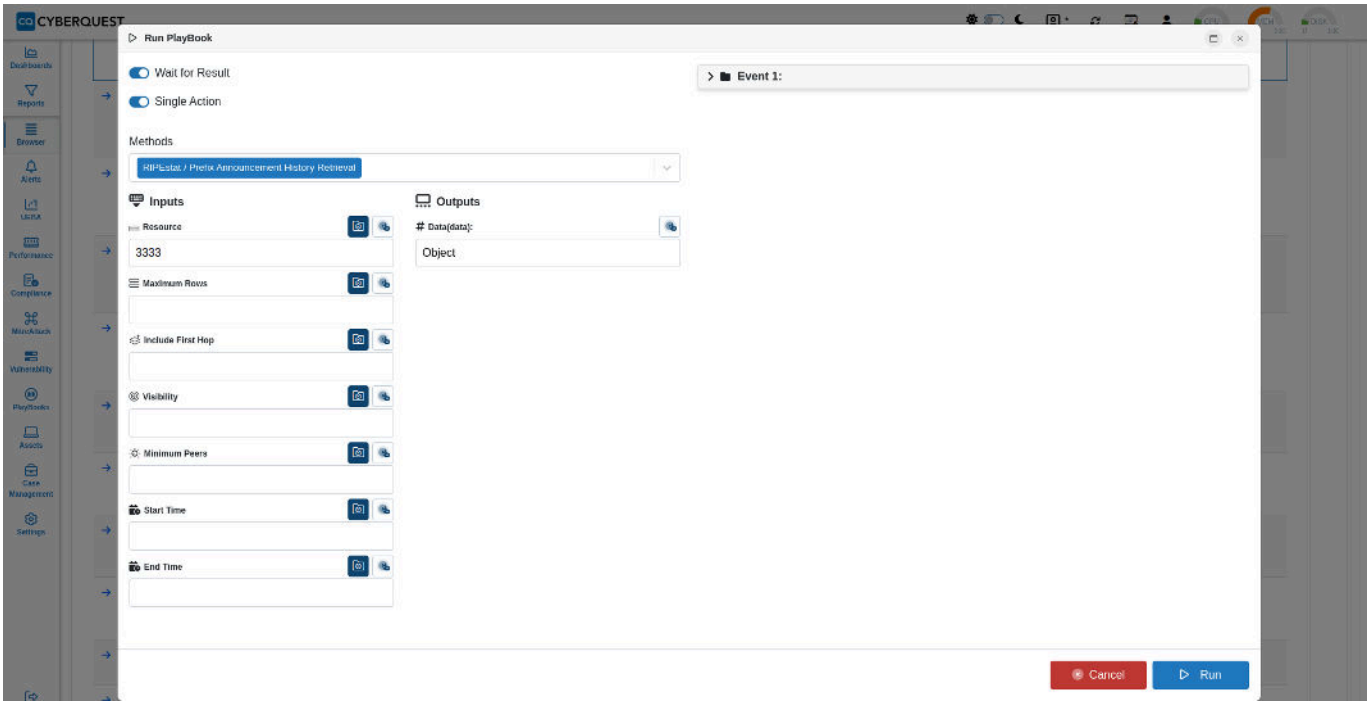


Inputs	Description
Resource (is required)	The resource to query. This is a prefix (v4/v6), IP address or AS number
Timestamp	Defines the time of the lookup. This value will be automatically aligned to a RIS collection time.
Minimum Peers Seeing	Minimum number of peers seeing the route for it to be included in the results. Excludes low-visibility/localized announcements.

Outputs	Description
Data (data)	The results of the API call

RIPEstat/Prefix Announcement History Retrieval method

This data call shows the history of announcements for prefixes, including the origin ASN and the first hop.

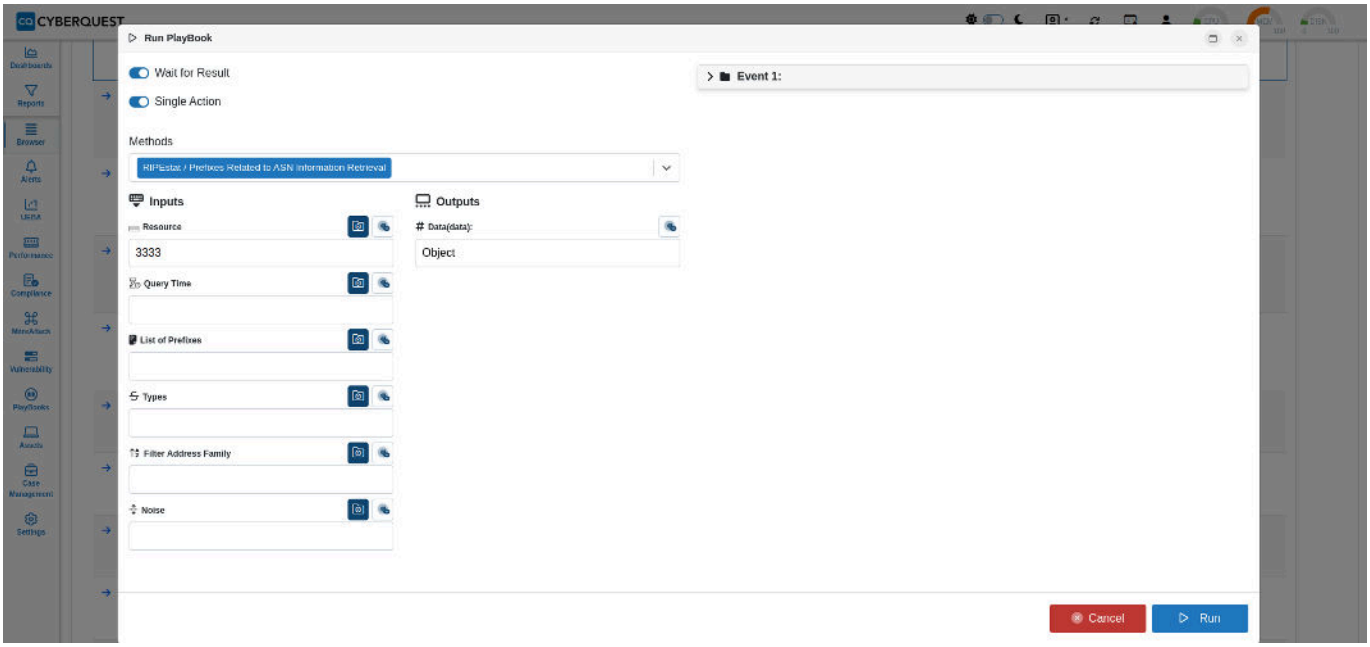


Inputs	Description
Resource (is required)	The resource to query. This is a prefix (v4/v6), IP address or AS number.
Maximum Rows	The maximum number of routes to return. This is a soft limit: all recorded routes for each origin ASN are returned, but when the row limit is reached no more origins will be returned.
Include First Hop	Include the first hop ASN in the route, instead of just the origin ASN
Visibility	Add a visibility field to each timeline indicating the visibility of the route (according to RIS) at that point in time. The visibility is computed as the peers_seeing divided by the number of RIS full table peers at the time.
Minimum Peers	Minimum number of full-feed RIS peers seeing the route for the segment to be included in the results. Excludes low-visibility/localized announcements.
Start Time	Defines the starttime for the query
End Time	Defines the endtime for the query

Outputs	Description
Data (data)	The results of the API call

RIPEstat/Prefixes Related to ASN Information Retrieval method

This data call provides information on prefixes related to an ASN. The data call distinguishes prefixes in the originated and transited ASN.

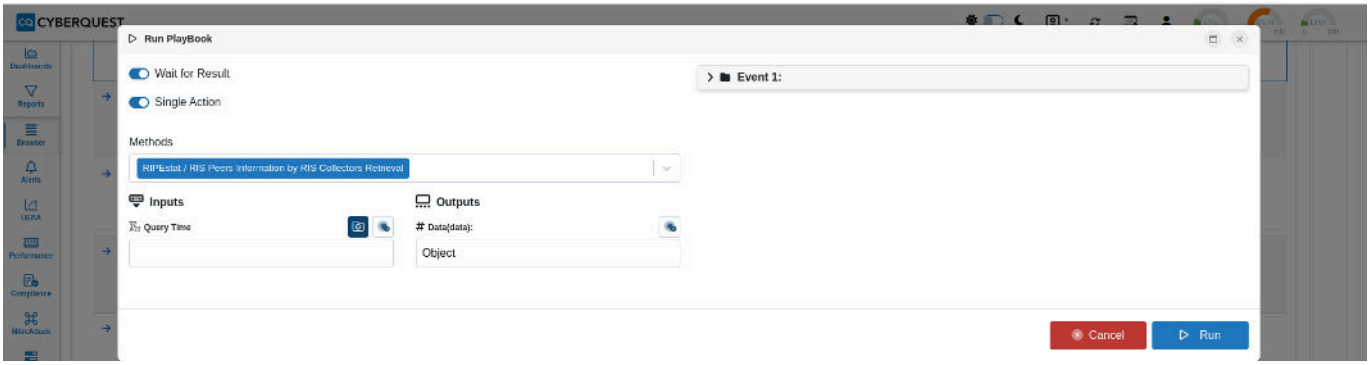


Inputs	Description
Resource (is required)	The ASN to be looked up.
Query Time	Defines the time of the lookup. This value needs to be aligned to the RIS dump times!
List of Prefixes	If true, the data call will return all prefixes and not only the total counts. This might be further separated into originating and transiting.
Types	o will show originating prefixes and t transiting. The combination shows both, which is the default.
Filter Address Family	This parameter lets you filter the address family: v4 shows only IPv4 and v6 only IPv6.
Noise	Noise refers to routed prefixes that are either coming from private IP space, single IP addresses or the entire IP space (/0). filter will remove these prefixes from the output, keep will not remove any prefixes.

Outputs	Description
Data (data)	The results of the API call

RIPEstat/RIS Peers Information by RIS Collectors Retrieval method

This data call provides information on the peers of RIS - ASN, IP address and number of shared routes. The data is grouped by RIS collectors.

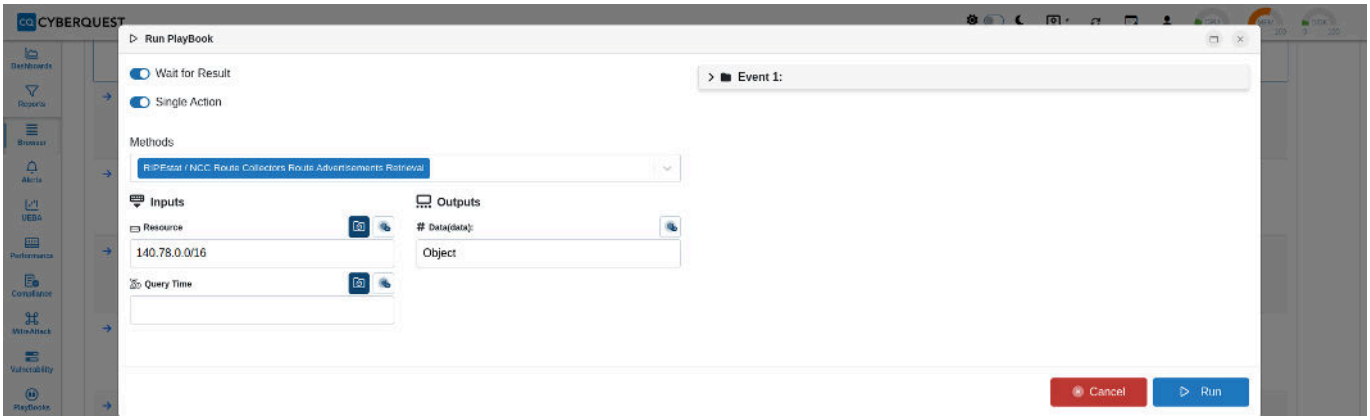


Inputs	Description
Query Time	Defines the time of the lookup. This value will be automatically aligned to a RIS collection time.

Outputs	Description
Data (data)	The results of the API call

RIPEstat/NCC Route Collectors Route Advertisements Retrieval method

This data call returns routes for advertisements of a given IP resource, or that are originated from a given ASN, as seen by the RIPE NCC route collectors.

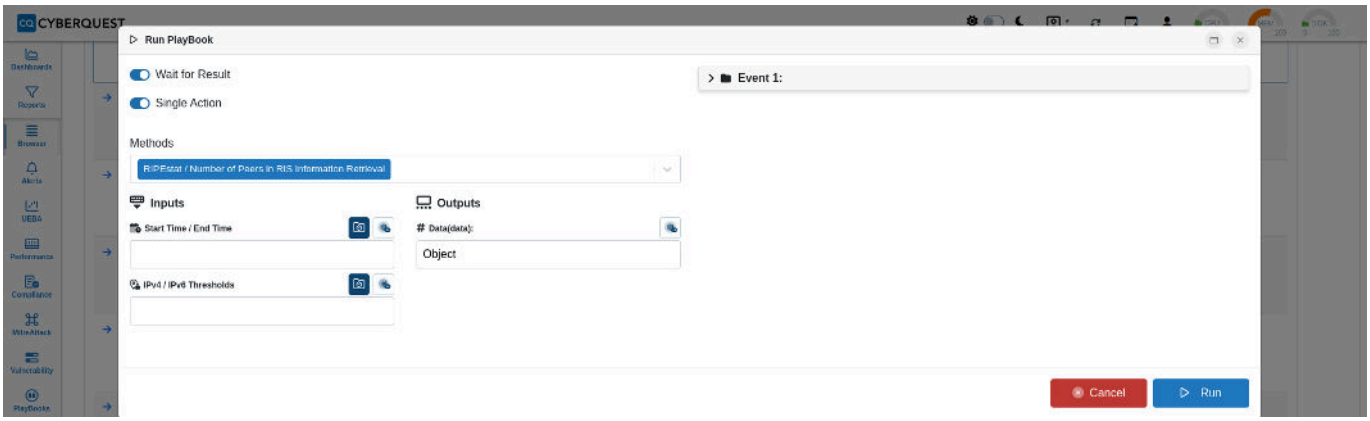


Inputs	Description
Resource (is required)	This is the resource the query is based on.
Query Time	Defines the time of the lookup. This value will be automatically aligned to a RIS collection time.

Outputs	Description
Data (data)	The results of the API call

RIPEstat/Number of Peers in RIS Information Retrieval method

This data call provides information on the number of peers as seen by RIS.

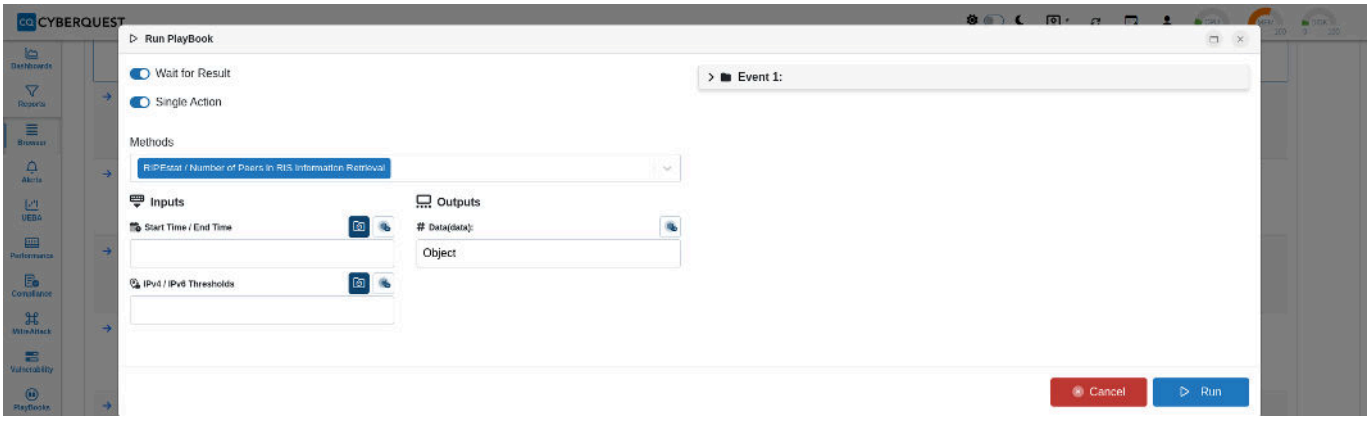


Inputs	Description
Start Time / End Time	Defines the start and end time for the query window
IPv4 / IPv6 Thresholds	Defines the thresholds (IPv4 and IPv6) used to calculate the number of full-table peers.

Outputs	Description
Data (data)	The results of the API call

RIPEstat/BGP Full-Table Peer Cut-Off Threshold Retrieval method

This data call provides the cut-off threshold for the number of prefixes that a BGP full-table peer requires to have. Peers to RIS that share less than this amount of prefixes are not considered full-table peers and hence are not considered in calculations like routing visibility. The threshold is obviously different between address families (IPv4 and IPv6) and time. For this reason the data call also supports historical lookups.

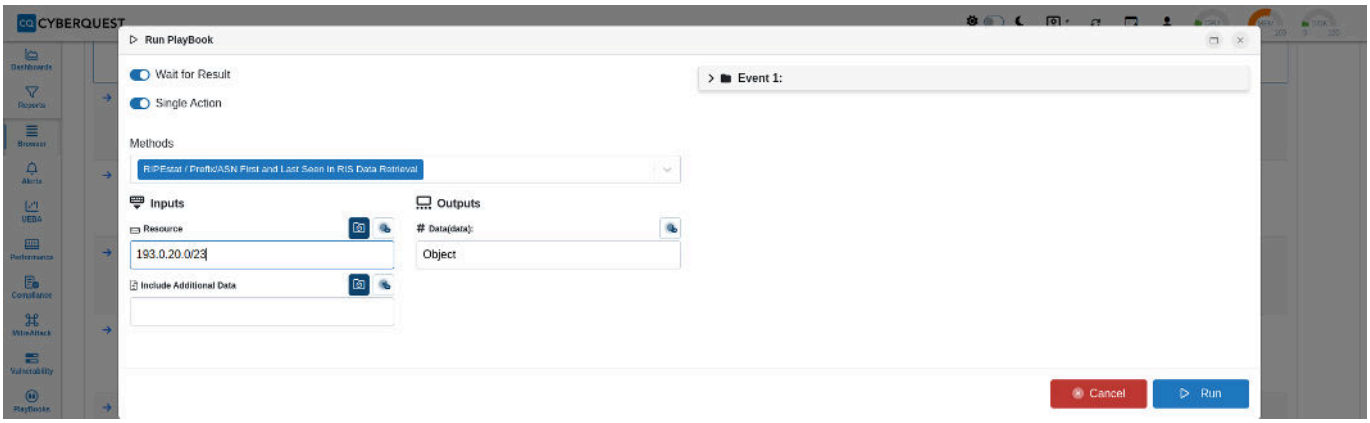


Inputs	Description
Query Time	Defines the time of the lookup. This value needs to be aligned to the RIS dump times (00:00, 08:00, 16:00) and will automatically be adjusted.

Outputs	Description
Data (data)	The results of the API call

RIPEstat/Prefix/ASN First and Last Seen in RIS Data Retrieval method

This data call provides information on when a prefix or ASN was first and last seen in RIS data.

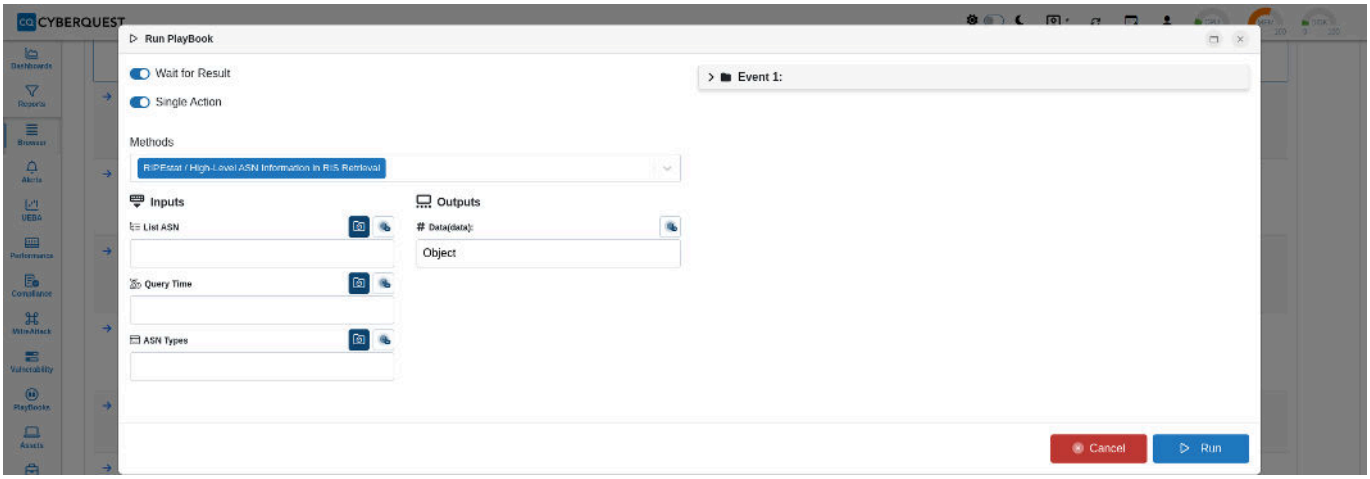


Inputs	Description
Resource (is required)	A prefix or ASN to be looked up.The output for ASNs distinguishes between how an ASN has been seen in RIS. This can be as either originating or not. Originating has the type set to o
Include Additional Data	This parameter defines additional data to be included.more_specific includes more specific IP ranges, which only works for prefix lookups. By default more_specific is not set as it makes the lookup slower.low_visibility_flag includes the flag to indicate low visibility. By default it is not included.

Outputs	Description
Data (data)	The results of the API call

RIPEstat/High-Level ASN Information in RIS Retrieval method

This data call provides high-level information on ASNs in RIS.

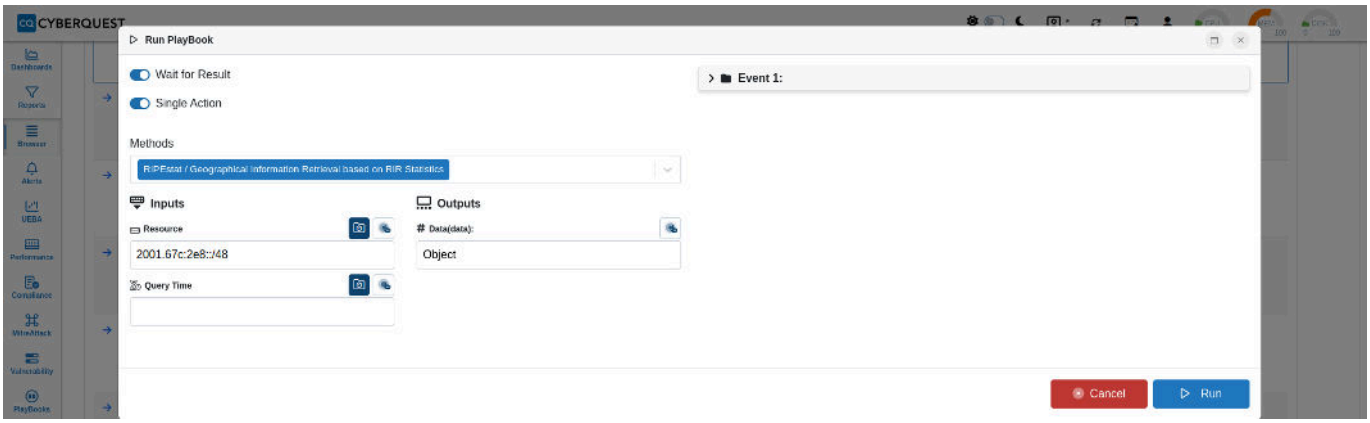


Inputs	Description
List ASN	If true, the data call will return a list of all ASNs. This might be further separated into originating and transiting.
Query Time	Defines the time of the lookup. This value needs to be aligned to the RIS dump times!
ASN Types	o stands for originating and will show originating ASNs separately. t does the same for transiting ASNs (keep in mind the definition of a transit in this case).

Outputs	Description
Data (data)	The results of the API call

RIPEstat/Geographical Information Retrieval based on RIR Statistics method

This data call returns geographical information for Internet resources based on RIR Statistics data.

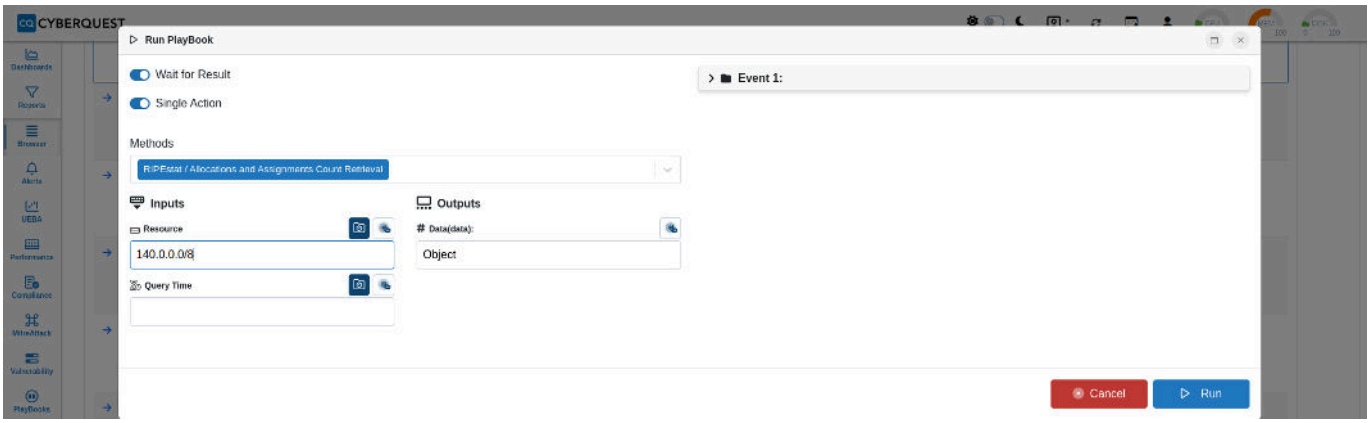


Inputs	Description
Resource (is required)	Defines the resource to be queried. For IP resource the result might be less or more specific to the given resource.
Query Time	Defines the times for the query; must be within the range of earliest_time and latest_time

Outputs	Description
Data (data)	The results of the API call

RIPEstat/Allocations and Assignments Count Retrieval method

This data call returns the number of allocations and assignments (below the queried resource) according to registration data provided by Regional Internet Registries.

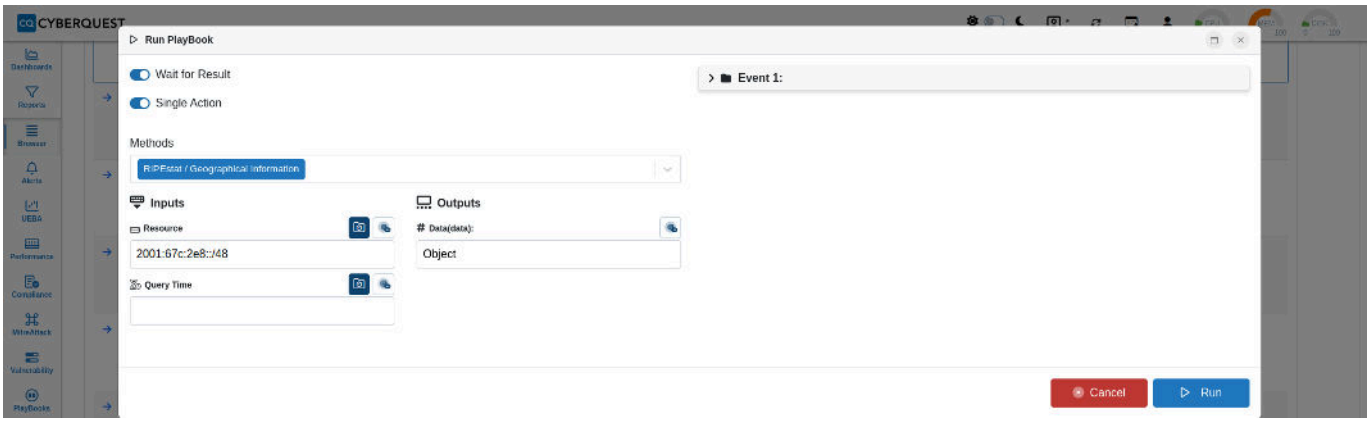


Inputs	Description
Resource (is required)	This is the resource the query is based on.
Query Time	Defines the query time

Outputs	Description
Data (data)	The results of the API call

RIPEstat/Geographical Information method

This data call returns geographical information for Internet resources based on RIR Statistics data.

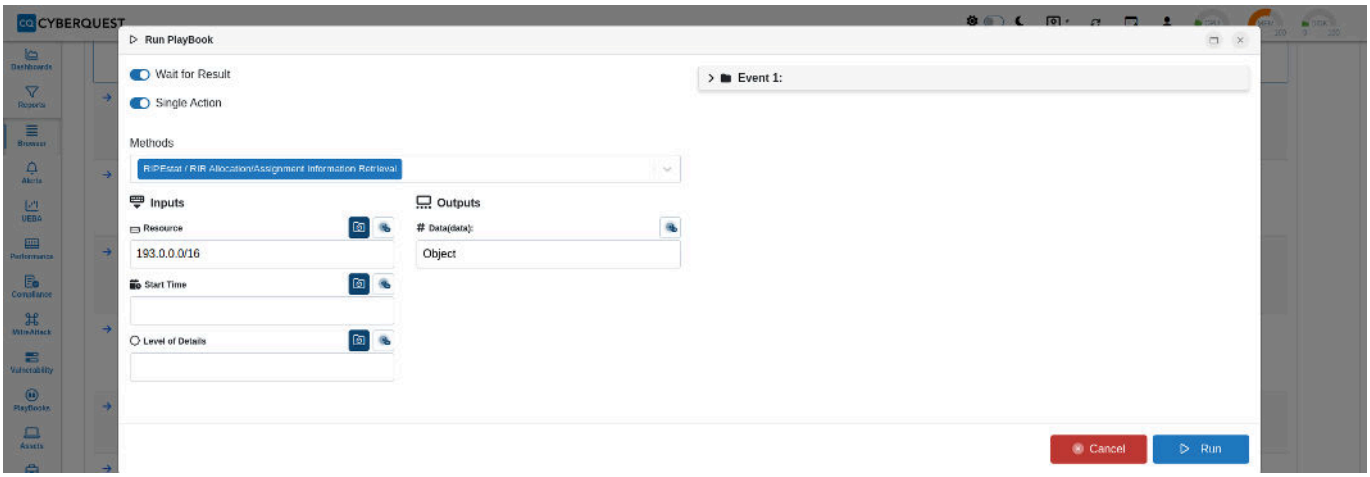


Inputs	Description
Resource (is required)	Defines the resource to be queried. For IP resource the result might be less or more specific to the given resource.
Query Time	Defines the times for the query; must be within the range of earliest_time and latest_time

Outputs	Description
Data (data)	The results of the API call

RIPEstat/RIR Allocation/Assignment Information Retrieval method

This data call shows which RIR(s) allocated/assigned a resource. Depending on the level of detail (lod parameter) this can include additional information like registration status or country of registration. The data is based on RIR stats files.

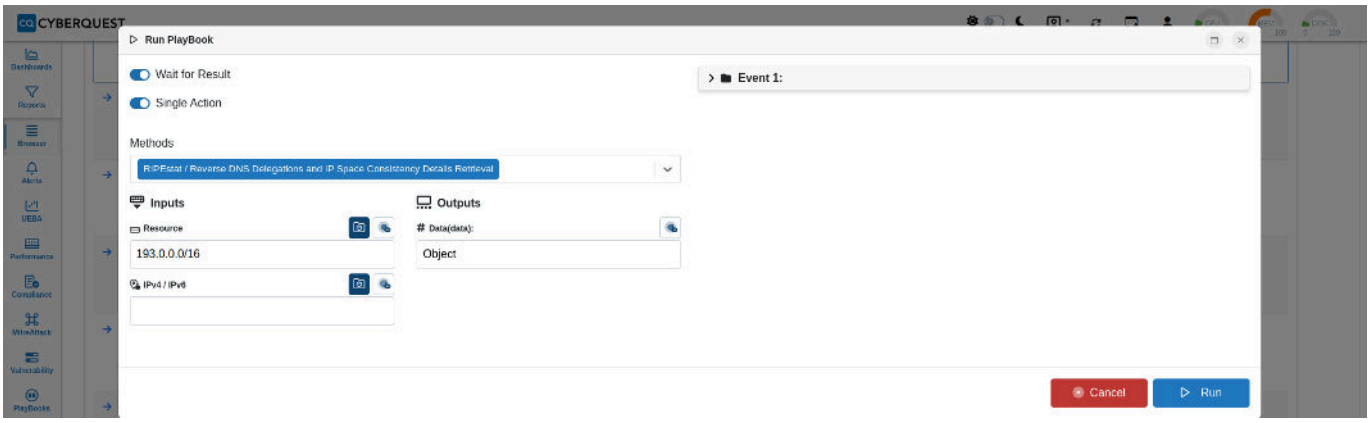


Inputs	Description
Resource (is required)	Defines the resource to be queried. The result contains resources that are more or less specific to the queried resource.
Start Time	Defines the time start and end time for the query.
Level of Details	Defines the level of detail in which the data is being returned.Levels are:* 0 - Least detailed output* 1 - Default output* 2 - Most detailed output

Outputs	Description
Data (data)	The results of the API call

RIPEstat/Reverse DNS Delegations and IP Space Consistency Details Retrieval method

This data call returns details on the reverse DNS delegations and its consistency with routed and registered IP space. The input can be a single prefix or an ASN, in which case all routed and registered prefixes for this ASN are used as an input.

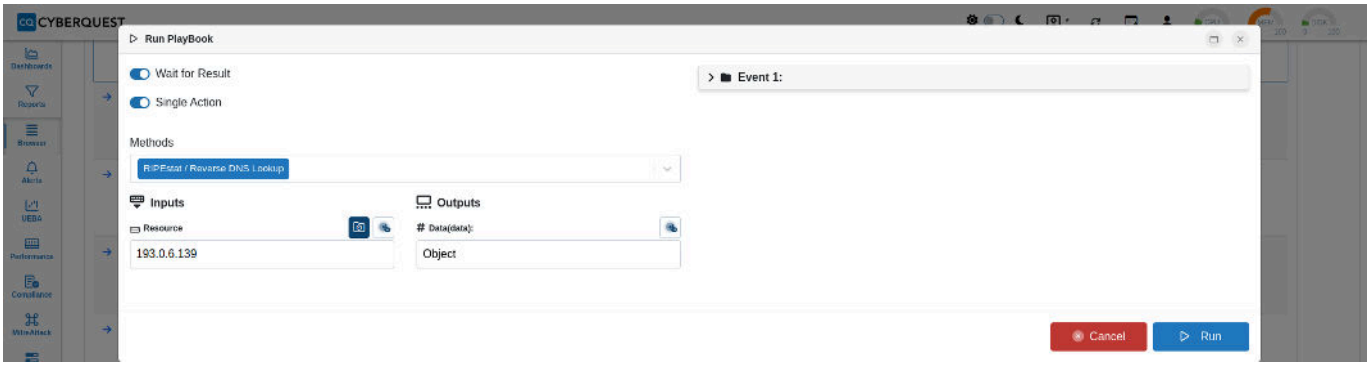


Inputs	Description
Resource (is required)	This is the resource the query is based on.
IPv4 / IPv6	Filter option on IP version

Outputs	Description
Data (data)	The results of the API call

RIPEstat/Reverse DNS Lookup method

This is just a simple lookup for the reverse DNS info against a single IP address.

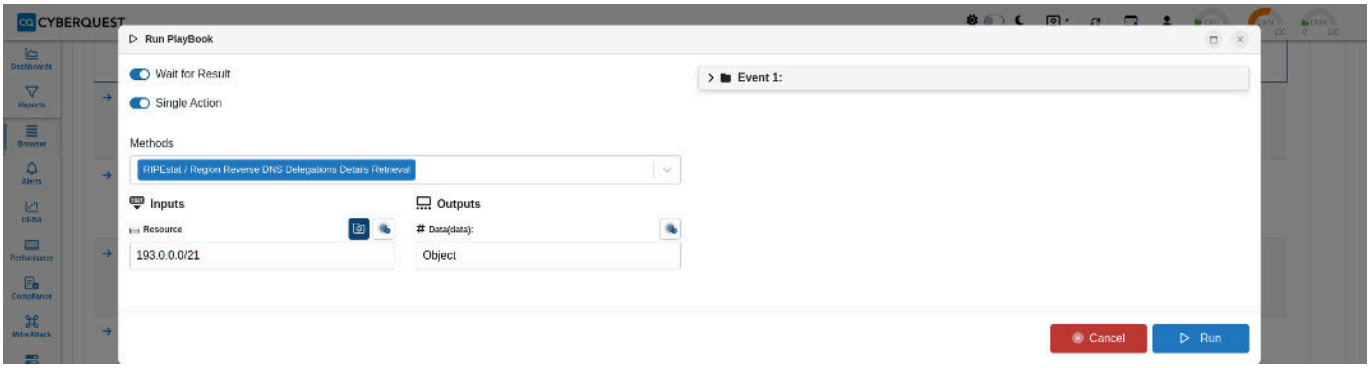


Inputs	Description
Resource (is required)	IP address for the query

Outputs	Description
Data (data)	The results of the API call

RIPEstat/Region Reverse DNS Delegations Details Retrieval method

This data call returns details of reverse DNS delegations for IP prefixes in the RIPE region.

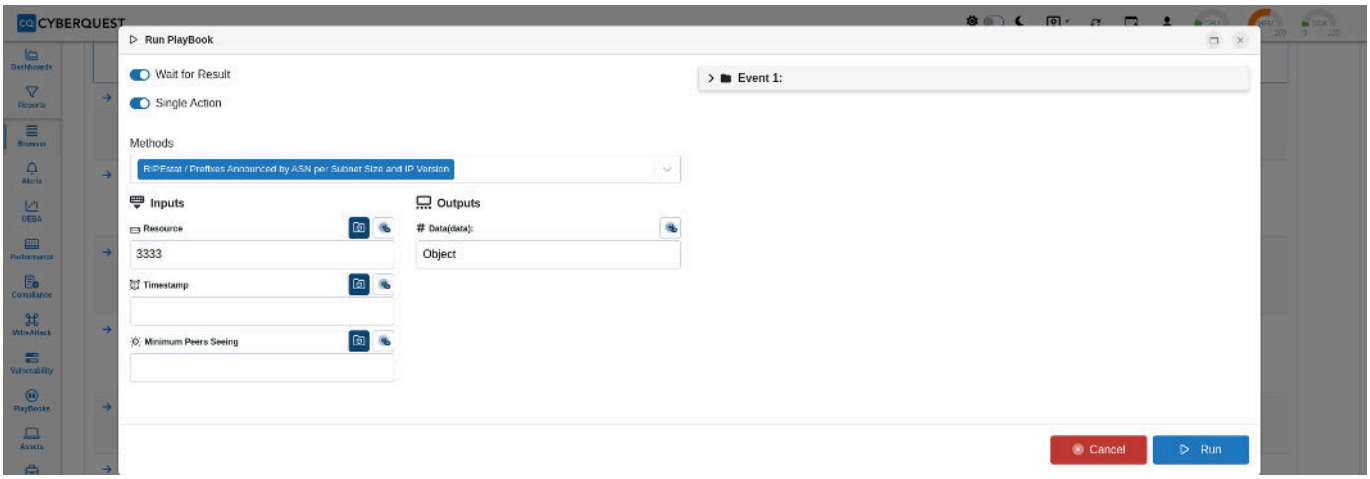


Inputs	Description
Resource (is required)	Prefix for the query

Outputs	Description
Data (data)	The results of the API call

RIPEstat/Prefixes Announced by ASN per Subnet Size and IP Version method

This data call returns the total amount of prefixes announced by a given ASN per subnet size and IP version.

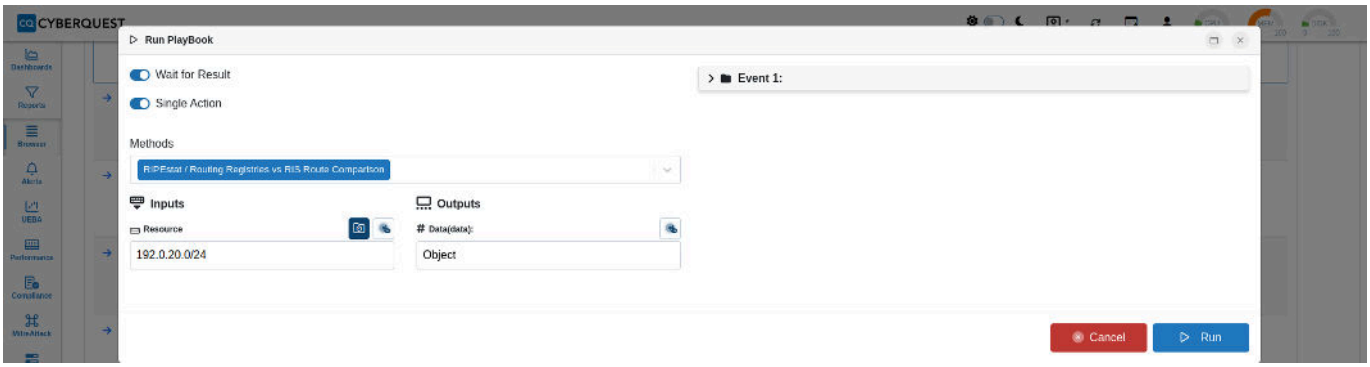


Inputs	Description
Resource (is required)	This is the resource the query is based on.
Timestamp	Defines the time for when to perform the query.
Minimum Peers Seeing	Minimum number of RIS peers seeing the prefix for it to be included in the results. Excludes low-visibility/localized announcements

Outputs	Description
Data (data)	The results of the API call

RIPEstat/Routing Registries vs RIS Route Comparison method

This data call compares the given routes (prefix originating from an ASN) between Routing Registries and actual routing behaviour as seen by the RIPE NCC route collectors (RIS).

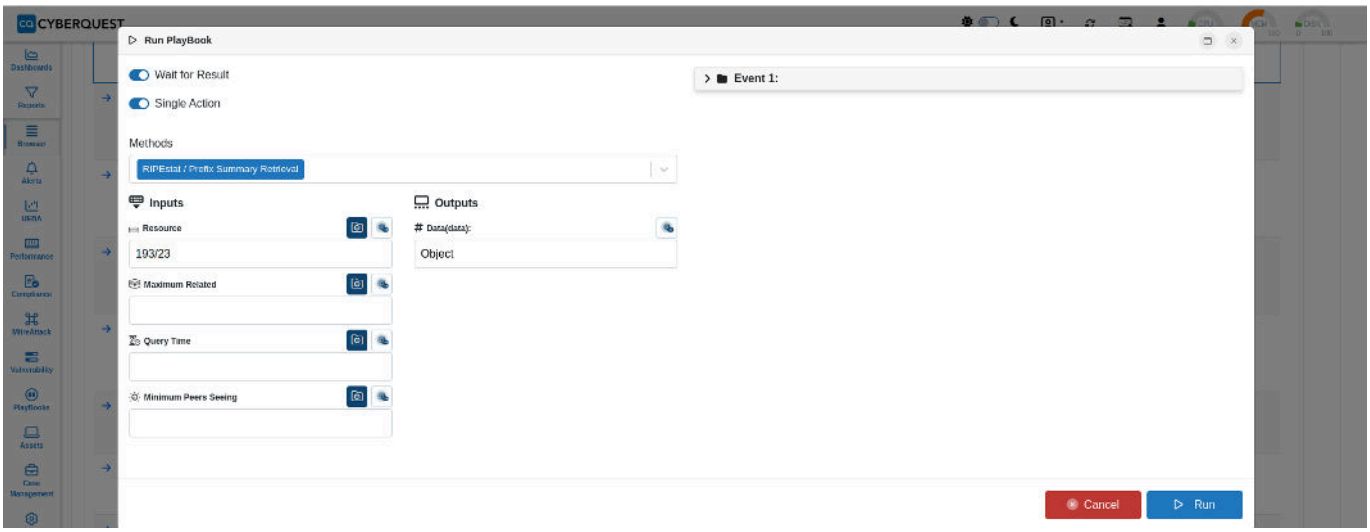


Inputs	Description
Resource (is required)	The prefix to query

Outputs	Description
Data (data)	The results of the API call

RIPEstat/Prefix Summary Retrieval method

This data call gives a summary of the given prefix, including whether and by whom it is announced.

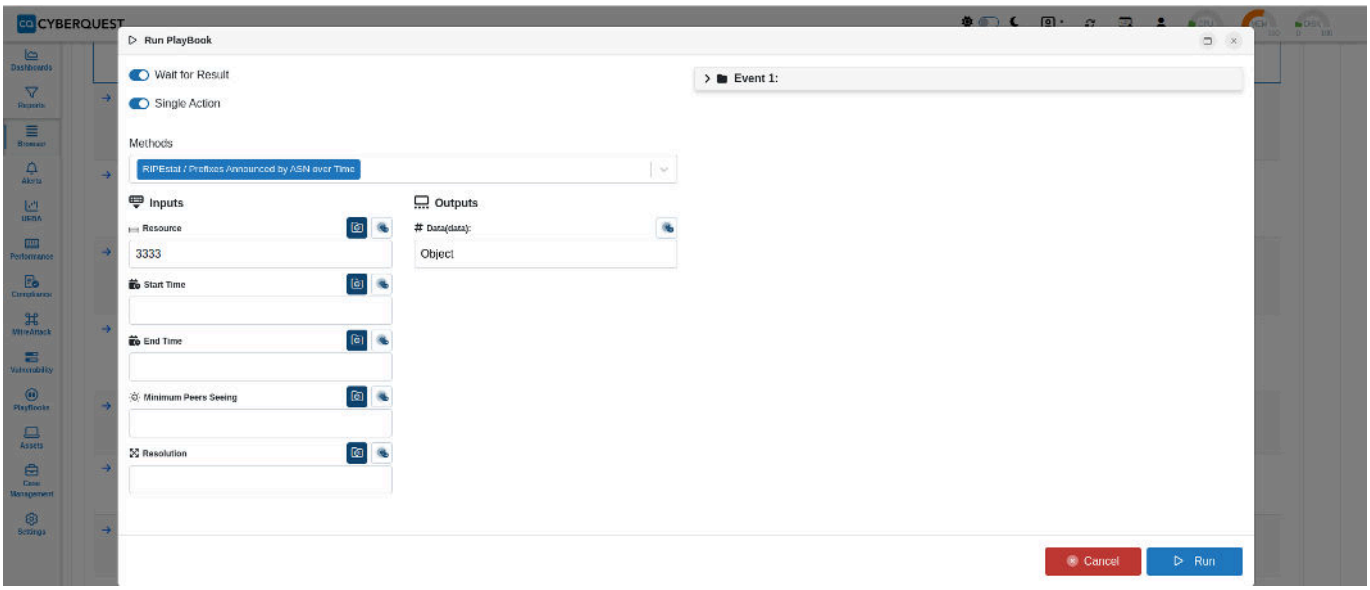


Inputs	Description
Resource (is required)	States the prefix you want to get the resource info for
Maximum Related	Limits the number of related prefixes - if there are any - included in the result
Query Time	Defines the query time for the lookup
Minimum Peers Seeing	Minimum number of (RIS) peers necessary to see a resource to be included in the result

Outputs	Description
Data (data)	The results of the API call

RIPEstat/Prefixes Announced by ASN over Time method

This data call shows the number of prefixes announced by a given ASN over time.

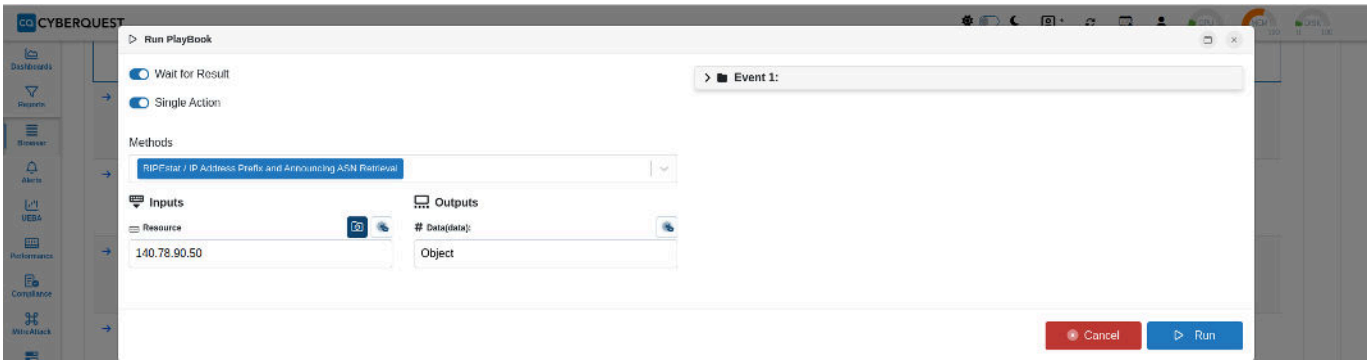


Inputs	Description
Resource (is required)	This is the resource the query is based on.
Start Time	Defines the start time for the query
End Time	Defines the endtime for the query
Minimum Peers Seeing	Minimum number of RIS peers seeing the prefix for it to be included in the results. Excludes low-visibility/localized announcements.
Resolution	Defines the resolution/aggregation for the returned data, e.g. 2d means that changes in the data must persist for longer than 2 days to be visible at this resolution.

Outputs	Description
Data (data)	The results of the API call

RIPEstat/IP Address Prefix and Announcing ASN Retrieval method

This data call returns the containing prefix and announcing ASN of a given IP address.

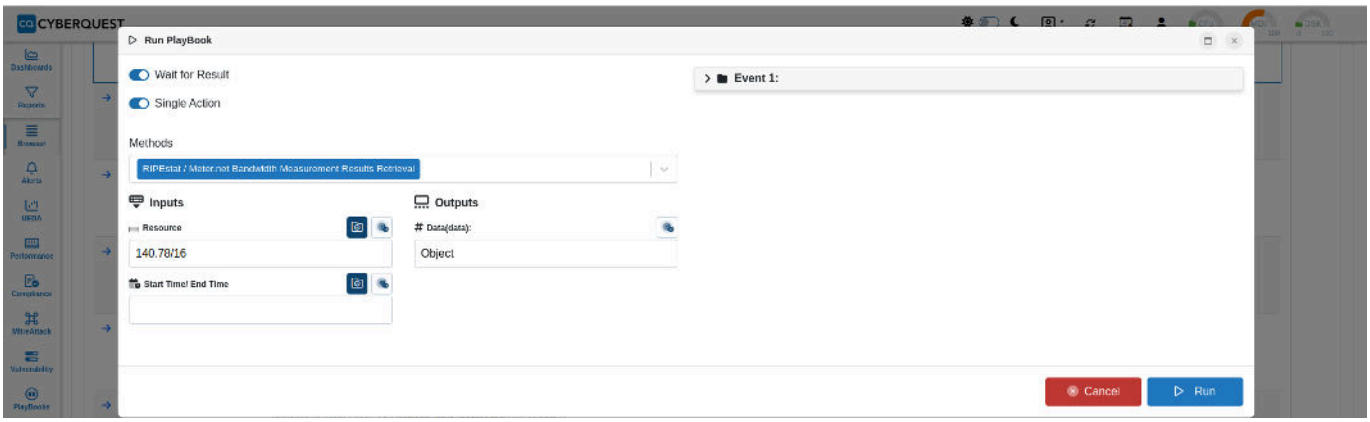


Inputs	Description
Resource (is required)	Any IP address one wants to get network info for

Outputs	Description
Data (data)	The results of the API call

RIPEstat/Meter.net Bandwidth Measurement Results Retrieval method

This data call returns bandwidth measurement results based on open data provided by meter.net.

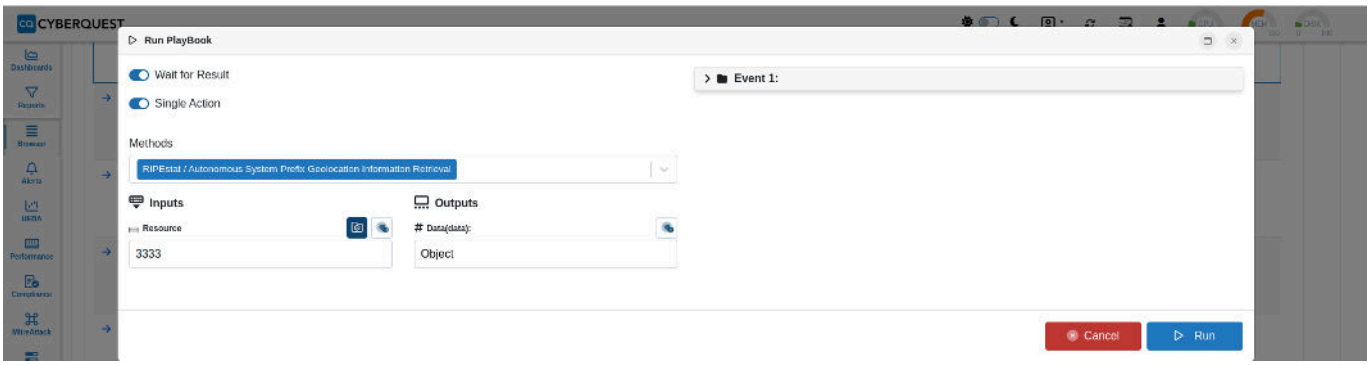


Inputs	Description
Resource (is required)	At this moment the data call only supports prefixes but aggregations for ASNs and countries is planned.
Start Time/ End Time	The start/end time defining the upper and lower boundary of the lookup.

Outputs	Description
Data (data)	The results of the API call

RIPEstat/Autonomous System Prefix Geolocation Information Retrieval method

This data call returns geolocation information for prefixes that are announced by an autonomous system.

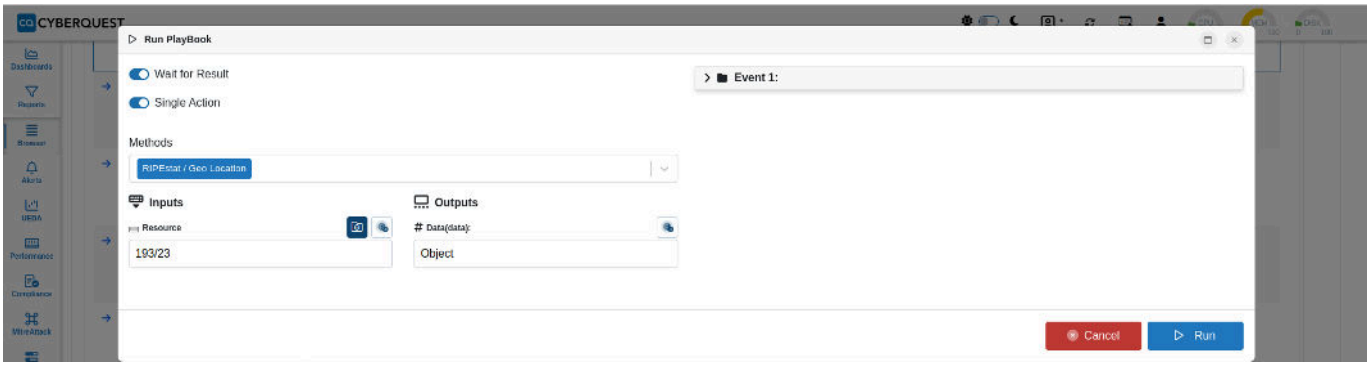


Inputs	Description
Resource (is required)	Number of the autonomous system

Outputs	Description
Data (data)	The results of the API call

RIPEstat/Geo Location method

This data call returns geolocation information for the given IP space based on MaxMinds GeoLite2 data source.

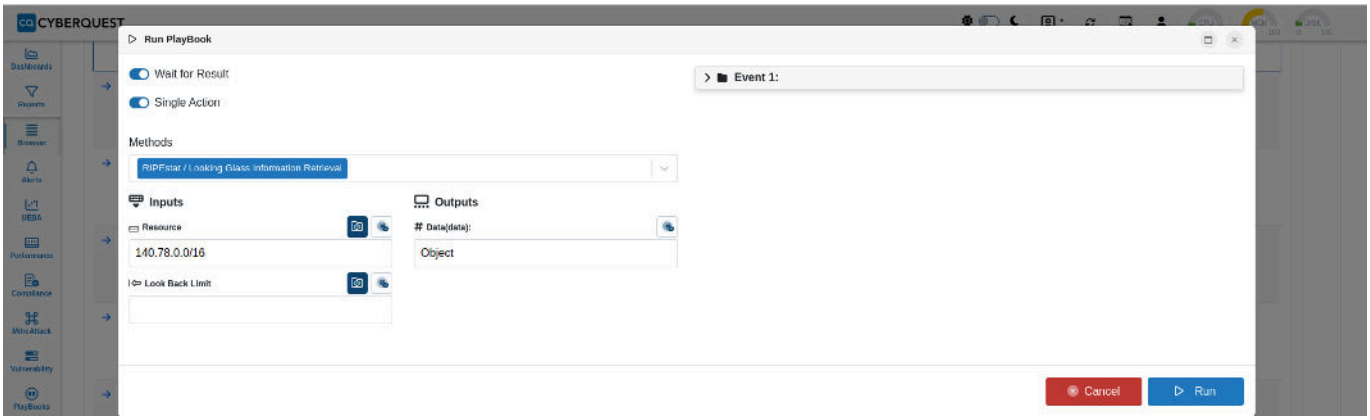


Inputs	Description
Resource (is required)	States the prefix or IP address you want to get the geographic information for

Outputs	Description
Data (data)	The results of the API call

RIPEstat/Looking Glass Information Retrieval method

This data call returns information coming from a Looking Glass.

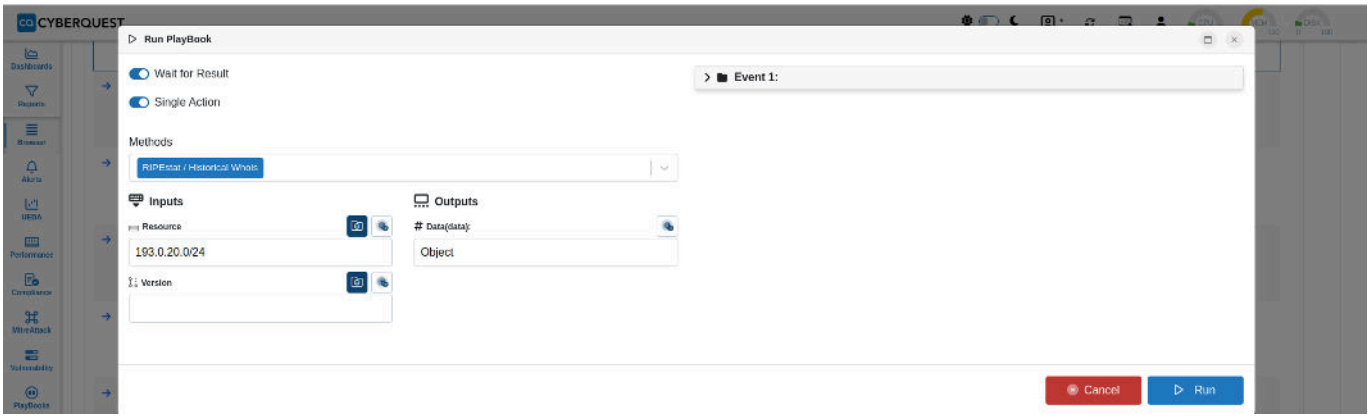


Inputs	Description
Resource (is required)	Prefixes need to match exactly a prefix found in the routing data. If given as IP address, the data call will try to find the encompassing prefix for the IP address.
Look Back Limit	Any results older than the cut-off threshold are not returned. This is useful when data is delayed and should not show up.

Outputs	Description
Data (data)	The results of the API call

RIPEstat/Historical Whois method

This data call provides information on objects that are stored in the RIPE DB. The result is aligned to a specific object, which is identified by an object type and an object key, which is similar to the Whois data call.

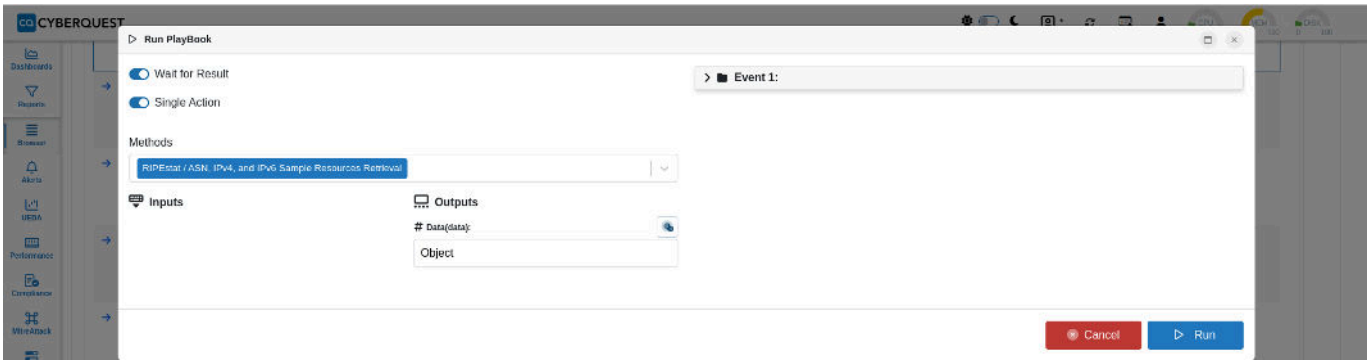


Inputs	Description
Resource (is required)	This is a prefix (v4/v6), an AS number, or a string of the format object-type:object-key for looking up generic database objects
Version	Given as a numerical value, the value must match exactly the historical version number.Given as a time-based value, the version that was valid at the given time will be returned.

Outputs	Description
Data (data)	The results of the API call

RIPEstat/ASN, IPv4, and IPv6 Sample Resources Retrieval method

This data call returns ASN, IPv4 and IPv6 sample resources.

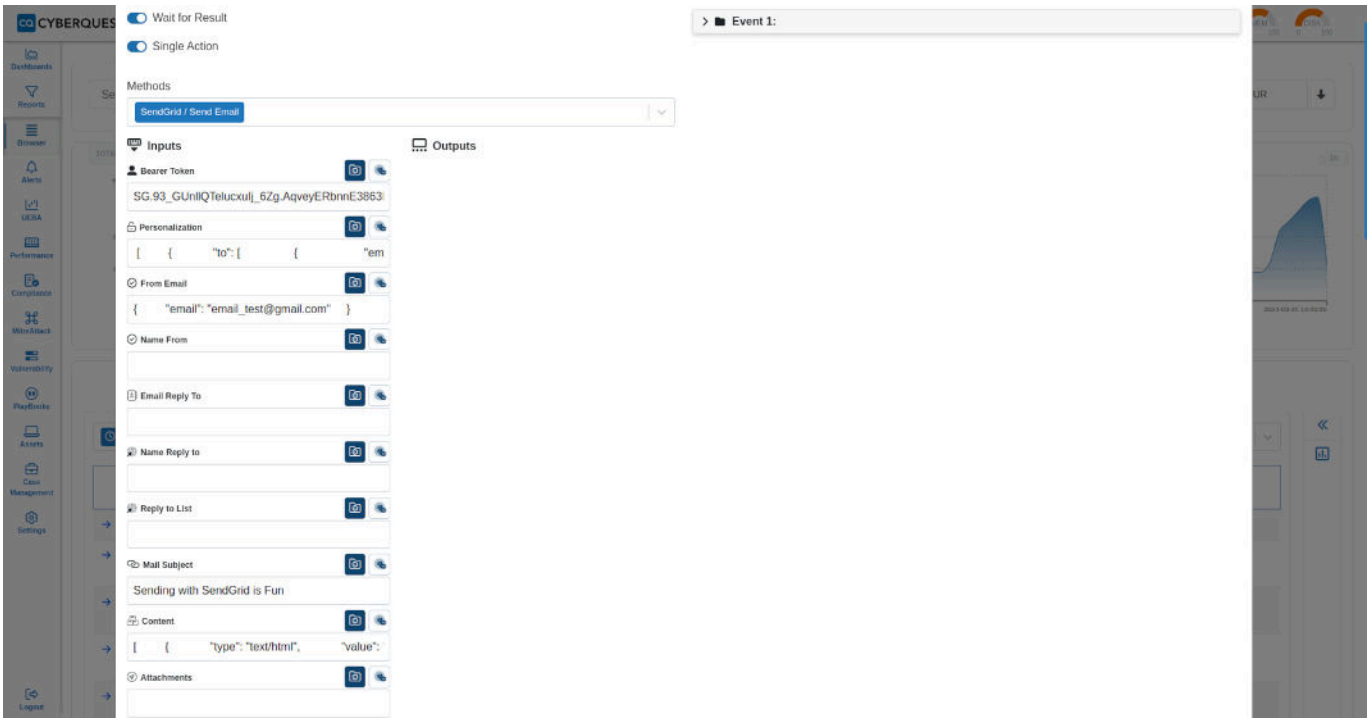


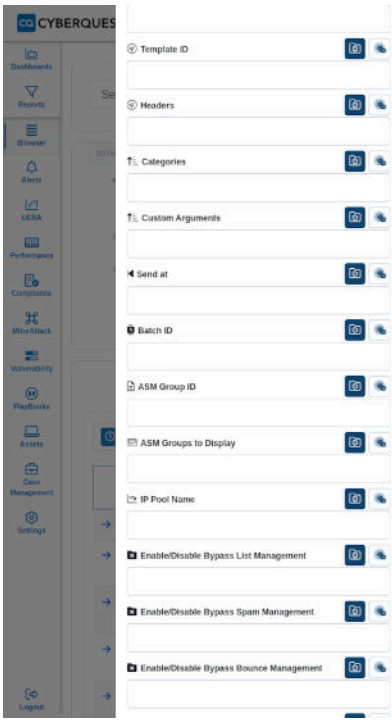
Outputs	Description
Data (data)	The results of the API call

SendGrid

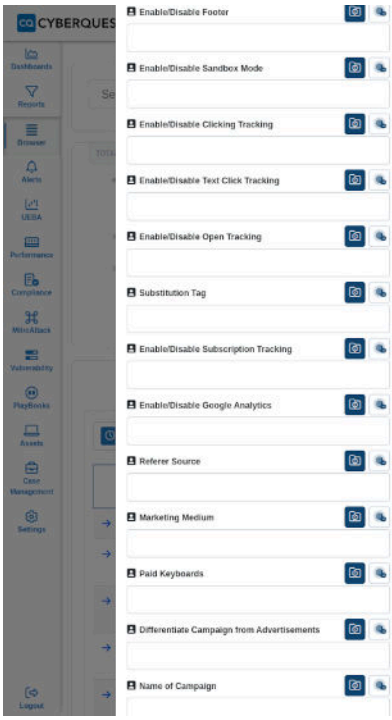
SendGrid/Send Email method

The Mail Send endpoint allows you to send email over SendGrid's v3 Web API.




Template ID
Headers
Categories
Custom Arguments
Send at
Batch ID
ASM Group ID
ASM Groups to Display
IP Pool Name
Enable/Disable Bypass List Management
Enable/Disable Bypass Spam Management
Enable/Disable Bypass Bounce Management




Enable/Disable Footer
Enable/Disable Sandbox Mode
Enable/Disable Clicking Tracking
Enable/Disable Text Click Tracking
Enable/Disable Open Tracking
Substitution Tag
Enable/Disable Subscription Tracking
Enable/Disable Google Analytics
Referer Source
Marketing Medium
Paid Keyboards
Differentiate Campaign from Advertisements
Name of Campaign



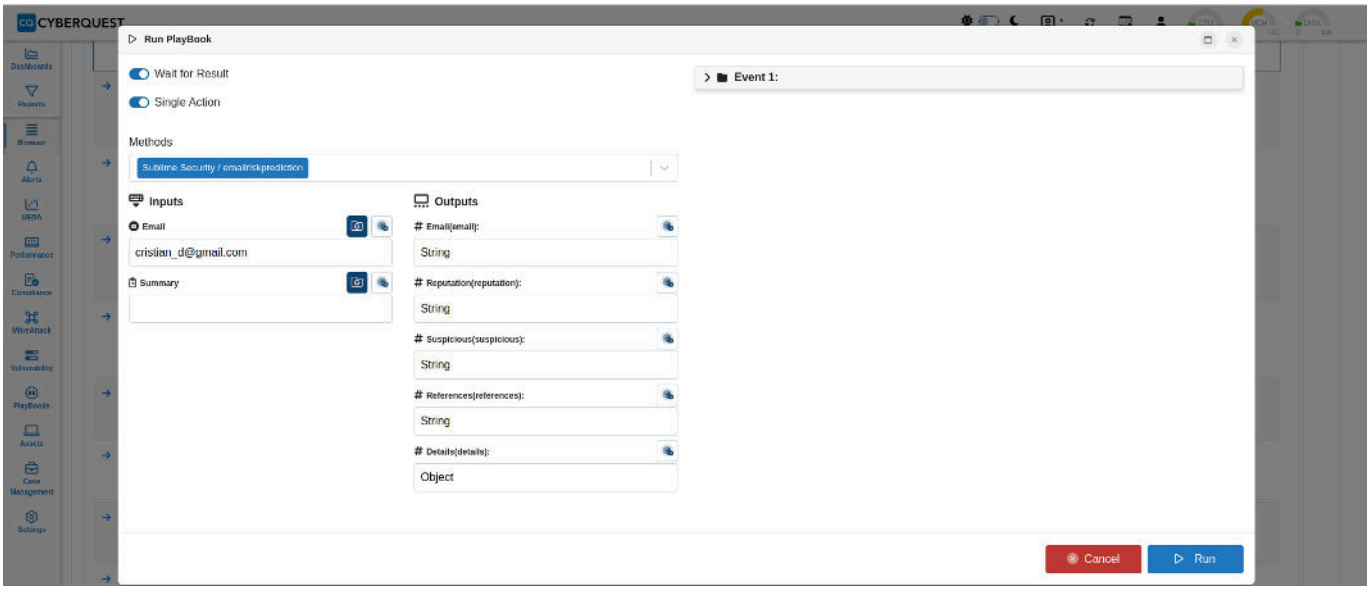
Inputs	Description
Bearer Token (is required)	Introduce Api key here
Personalization (is required)	An array of messages and their metadata. Each object within personalizations can be thought of as an envelope - it defines who should receive an individual message and how that message should be handled.
From Email (is required)	The From email address used to deliver the message. This address should be a verified sender in your Twilio SendGrid account
Name From	A name or title associated with the sending email address.
Email Reply To	The email address where any replies will be sent.
Name Reply to	A name or title associated with the reply_to email address.
Reply to List	An array of recipients who will receive replies. Each object in this array must contain the recipients email address. Each object in the array may optionally contain the recipients name. You can either choose to use “reply_to” field or “reply_to_list” but not both.
Mail Subject (is required)	The global or message level subject of your email. This may be overridden by subject lines set in personalizations.
Content (is required)	An array where you can specify the content of your email. You can include multiple MIME types of content, but you must specify at least one MIME type. To include more than one MIME type, add another object to the array containing the type and value parameters.
Attachments	An array of objects where you can specify any attachments you want to include
Template ID	An email template ID. A template that contains a subject and content — either text or html — will override any subject and content values specified at the personalizations or message level.
Headers	An object containing key/value pairs of header names and the value to substitute for them. The key/value pairs must be strings. You must ensure these are properly encoded if they contain unicode characters. These headers cannot be one of the reserved headers.
Categories	An array of category names for this message. Each category name may not exceed 255 characters.
Custom Arguments	Values that are specific to the entire send that will be carried along with the email and its activity data. Key/value pairs must be strings. Substitutions will not be made on custom arguments, so any string that is entered into this parameter will be assumed to be the custom argument that you would like to be used. This parameter is overridden by custom_args set at the personalizations level. Total custom_args size may not exceed 10,000 byte
Send at	A unix timestamp allowing you to specify when you want your email to be delivered. This may be overridden by the send_at parameter set at the personalizations level. Delivery cannot be scheduled more than 72 hours in advance. If you have the flexibility, its better to schedule mail for off-peak times. Most emails are scheduled and sent at the top of the hour or half hour. Scheduling email to avoid peak times — for example, scheduling at 10:53 — can result in lower deferral rates due to the reduced traffic during off-peak times.
Batch ID	An ID representing a batch of emails to be sent at the same time. Including a batch_id in your request allows you include this email in that batch. It also enables you to cancel or pause the delivery of that batch. For more information, see the Cancel Scheduled Sends API.
ASM Group ID	The unsubscribe group to associate with this email.
ASM Groups to Display	An array containing the unsubscribe groups that you would like to be displayed on the unsubscribe preferences page.
IP Pool Name	The IP Pool that you would like to send this email from.
Enable/Disable Bypass List Management	Allows you to bypass all unsubscribe groups and suppressions to ensure that the email is delivered to every single recipient. This should only be used in emergencies when it is absolutely necessary that every recipient receives your email. This filter cannot be combined with any other bypass filters.
Enable/Disable Bypass Spam Management	Allows you to bypass the spam report list to ensure that the email is delivered to recipients. Bounce and unsubscribe lists will still be checked; addresses on these other lists will not receive the message. This filter cannot be combined with the bypass_list_management filter. See our documentation for more about bypass filters. Indicates if this setting is enabled.

Inputs	Description
Enable/Disable Bypass Bounce Management	Allows you to bypass the bounce list to ensure that the email is delivered to recipients. Spam report and unsubscribe lists will still be checked; addresses on these other lists will not receive the message. This filter cannot be combined with the bypass_list_managementIndicates if this setting is enabled.
Enable/Disable Bypass Bounce Management	Allows you to bypass the global unsubscribe list to ensure that the email is delivered to recipients. Bounce and spam report lists will still be checked; addresses on these other lists will not receive the message. This filter applies only to global unsubscribes and will not bypass group unsubscribes. This filter cannot be combined with the bypass_list_management filter. Indicates if this setting is enabled.
Enable/Disable Footer	Optional. The contributors username.
Enable/Disable Sandbox Mode	Optional. The contributors username.
Enable/Disable Clicking Tracking	Allows you to track if a recipient clicked a link in your email. Indicates if this setting is enabled.
Enable/Disable Text Click Tracking	Allows you to track if a recipient clicked a link in your email. Indicates if this setting should be included in the text/plain portion of your email
Enable/Disable Open Tracking	Allows you to track if the email was opened by including a single pixel image in the body of the content. When the pixel is loaded, Twilio SendGrid can log that the email was opened.Indicates if this setting is enabled.
Substitution Tag	Allows you to track if the email was opened by including a single pixel image in the body of the content. When the pixel is loaded, Twilio SendGrid can log that the email was opened.Allows you to specify a substitution tag that you can insert in the body of your email at a location that you desire. This tag will be replaced by the open tracking pixel
Enable/Disable Subscription Tracking	Allows you to insert a subscription management link at the bottom of the text and HTML bodies of your email. If you would like to specify the location of the link within your email, you may use the substitution_tag.Indicates if this setting is enabled.
Enable/Disable Google Analytics	Allows you to enable tracking provided by Google Analytics.Indicates if this setting is enabled.
Referer Source	Name of the referrer source. (e.g. Google, SomeDomain.com, or Marketing Email)
Marketing Medium	Name of the marketing medium. (e.g. Email)
Paid Keyboards	Used to identify any paid keywords
Differentiate Campaign from Advertisements	Used to differentiate your campaign from advertisements.
Name of Campaign	The name of the campaign.

Sublime Security

Sublime Security /emailriskprediction method

EmailRep uses hundreds of data points from social media profiles, professional networking sites, dark web credential leaks, data breaches, phishing kits, phishing emails, spam lists, open mail relays, domain age and reputation, deliverability, and more to predict the risk of an email address.



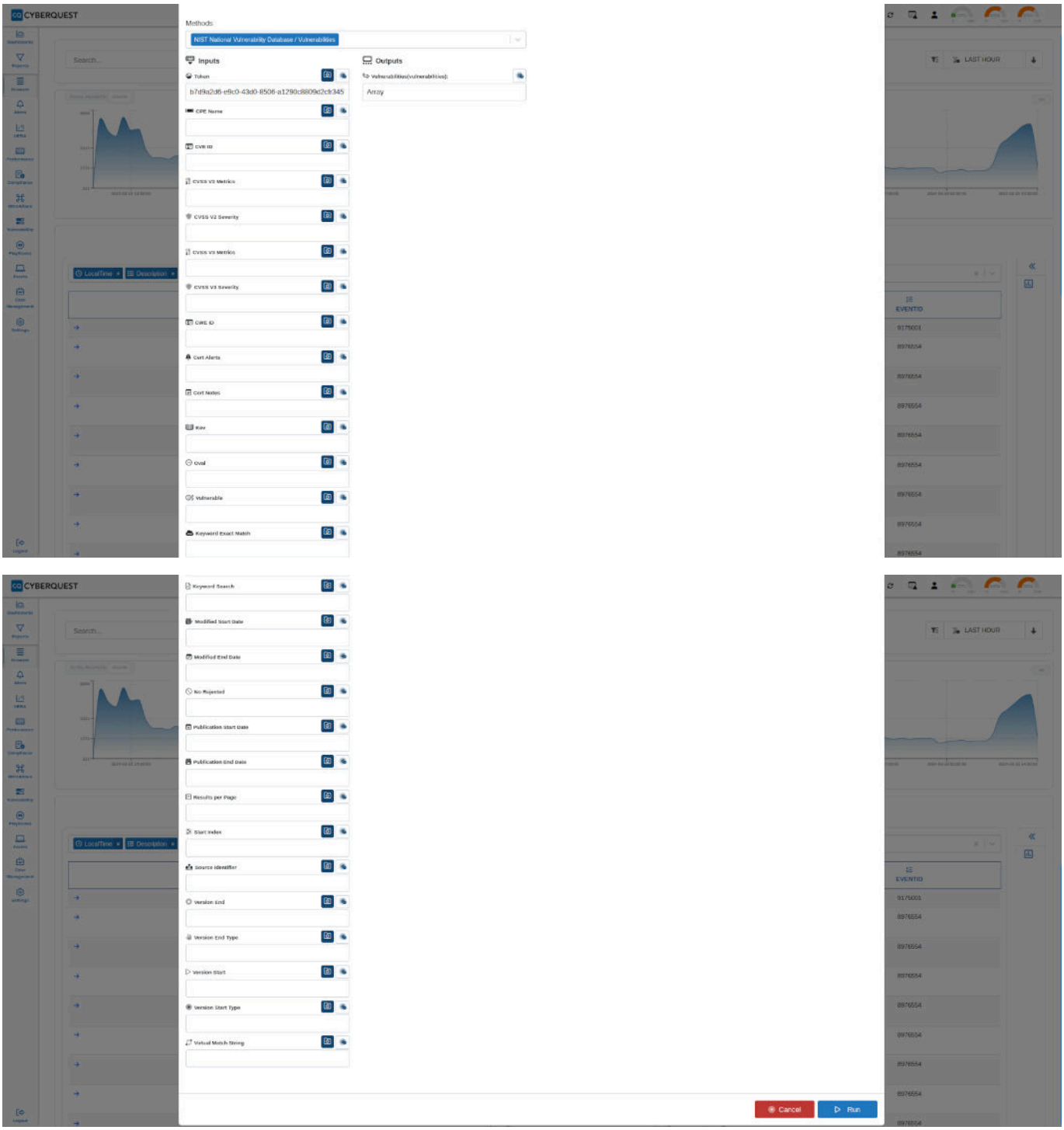
Inputs	Description
Email (is required)	Email address being queried
Summary	Return human-readable summary

Outputs	Description
Email (email)	Email address queried
Reputation (reputation)	high/medium/low/none
Suspicious (suspicious)	Whether the email address should be treated as suspicious or risky
References (references)	total number of positive and negative sources of reputation. note that these may not all be direct references to the email address, but can include reputation sources for the domain or other related information
Details (details)	Additional details about the investigated email

The NIST National Vulnerability Database

NIST National Vulnerability Database/Vulnerabilities method

The CVE API is used to easily retrieve information on a single CVE or a collection of CVE from the NVD.


CYBERQUEST
Methods:
NIST National Vulnerability Database / Vulnerabilities
Inputs
Outputs
Token
b7d9a2d6-e6c0-43d0-8506-a1290c8809d2ctk345
Array
CPE Name
CVE ID
CVSS V2 Metrics
CVSS V2 Severity
CVSS V3 Metrics
CVSS V3 Severity
CWE ID
Cert Alerts
Cert Notes
Kev
Oval
Vulnerable
Keyword Exact Match
Keyword Search
Modified Start Date
Modified End Date
No Rejected
Publication Start Date
Publication End Date
Results per Page
Start Index
Source Identifier
Version End
Version End Type
Version Start
Version Start Type
Virtual Match String
Cancel
Run
LAST HOUR

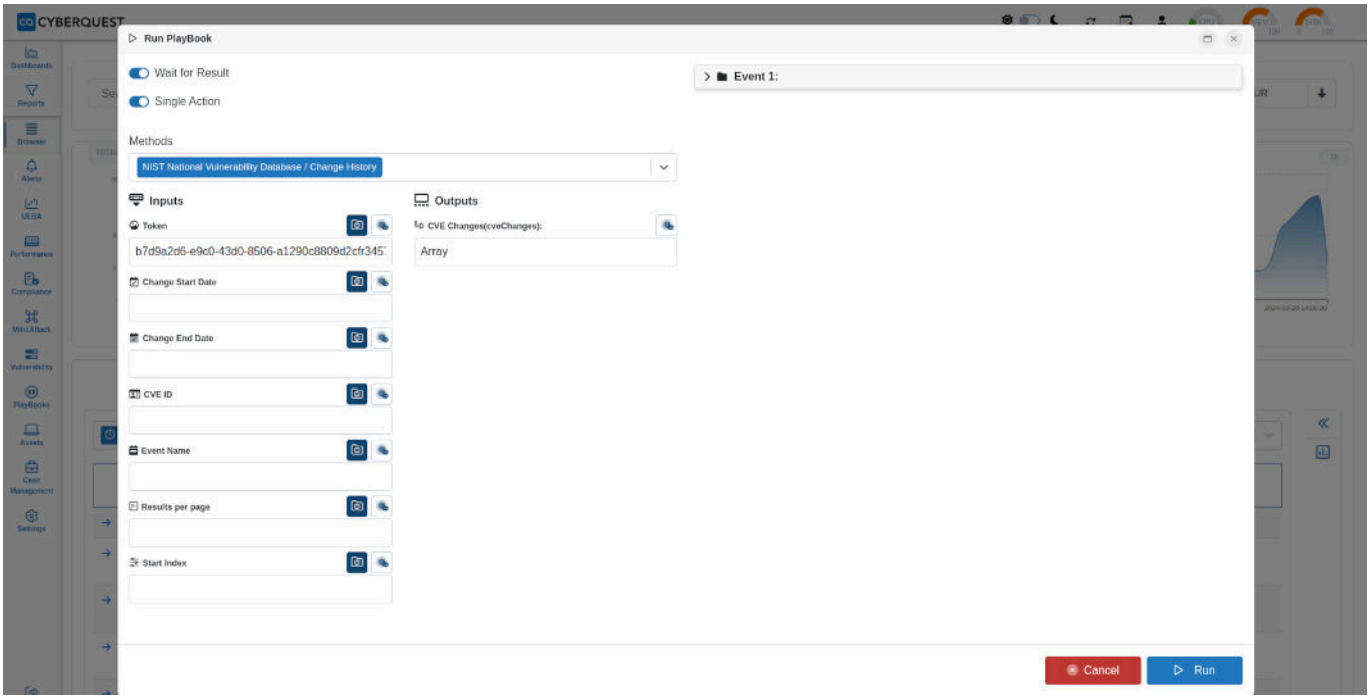
Inputs	Description
Token (is required)	To use the NIST National Vulnerability Database API, you must have an API key.
CPE Name	This parameter returns all CVE associated with a specific CPE. The exact value provided with cpeName is compared against the CPE Match Criteria within a CVE applicability statement. If the value of cpeName is considered to match, the CVE is included in the results.
CVE ID	This parameter returns a specific vulnerability identified by its unique Common Vulnerabilities and Exposures identifier (the CVE ID). cveId will not accept {CVE-ID} for vulnerabilities not yet published in the NVD
CVSS V2 Metrics	This parameter returns only the CVEs that match the provided CVSS V2 Metrics
CVSS V2 Severity	This parameter returns only the CVEs that match the provided CVSSv2 qualitative severity rating
CVSS V3 Metrics	This parameter returns only the CVEs that match the provided CVSS V3 Metrics
CVSS V3 Severity	Host to submit
CWE ID	This parameter returns only the CVE that include a weakness identified by Common Weakness Enumeration using the provided {CWE-ID}
Cert Alerts	This parameter returns the CVE that contain a Technical Alert from US-CERT
Cert Notes	This parameter returns the CVE that contain a Vulnerability Note from CERT/CC.
Kev	This parameter returns the CVE that appear in CISAs Known Exploited Vulnerabilities (KEV) Catalog
Oval	This parameter returns the CVE that contain information from MITREs Open Vulnerability and Assessment Language (OVAL) before this transitioned to the Center for Internet Security (CIS).
Vulnerable	This parameter returns only CVE associated with a specific CPE, where the CPE is also considered vulnerable.
Keyword Exact Match	By default, this parameter returns any CVE where a word or phrase is found in the current description
Keyword Search	This parameter returns only the CVEs where a word or phrase is found in the current description.
Modified Start Date	These parameters return only the CVEs that were last modified during the specified period (Modified Start Date and Modified End Date)
Modified End Date	These parameters return only the CVEs that were last modified during the specified period (Modified Start Date and Modified End Date)
No Rejected	By default, the CVE API includes CVE records with the REJECT or Rejected status. This parameter excludes CVE records with the REJECT or Rejected status from API response.
Publication Start Date	These parameters return only the CVEs that were added to the NVD (i.e., published) during the specified period. If filtering by the published date, both Publication Start Date and Publication End Date are REQUIRED. The maximum allowable range when using any date range parameters is 120 consecutive days.
Publication End Date	These parameters return only the CVEs that were added to the NVD (i.e., published) during the specified period. If filtering by the published date, both Publication Start Date and Publication End Date are REQUIRED. The maximum allowable range when using any date range parameters is 120 consecutive days.
Results per Page	This parameter specifies the maximum number of CVE records to be returned in a single API response. For network considerations, the default value and maximum allowable limit is 2,000
Start Index	This parameter specifies the index of the first CVE to be returned in the response data.
Source Identifier	his parameter returns CVE where the exact value of Source Identifier appears as a data source in the CVE record.
Version End	The Virtual Match String parameter may be combined with Version and Version End Type to return only the CVEs associated with CPEs in specific version ranges.NaN

Inputs	Description
Version End Type	The Virtual Match String parameter may be combined with Version and Version End Type to return only the CVEs associated with CPEs in specific version ranges.NaN
Version Start	The Virtual Match String parameter may be combined with Version Start and Version Start Type to return only the CVEs associated with CPEs in specific version ranges.NaN
Version Start Type	The Virtual Match String parameter may be combined with Version Start and Version Start Type to return only the CVEs associated with CPEs in specific version ranges.NaN
Virtual Match String	Host to submit

Outputs	Description
Vulnerabilities (vulnerabilities)	The Vulnerabilities object contains an array of objects equal to the number of CVE returned in the response and is sorted in ascending order by the published property of the cve object. The cve object is explained in more detail below

NIST National Vulnerability Database/Change History method

The CVE Change History API is used to easily retrieve information on changes made to a single CVE or a collection of CVE from the NVD. This API provides additional transparency to the work of the NVD, allowing users to easily monitor when and why vulnerabilities change.

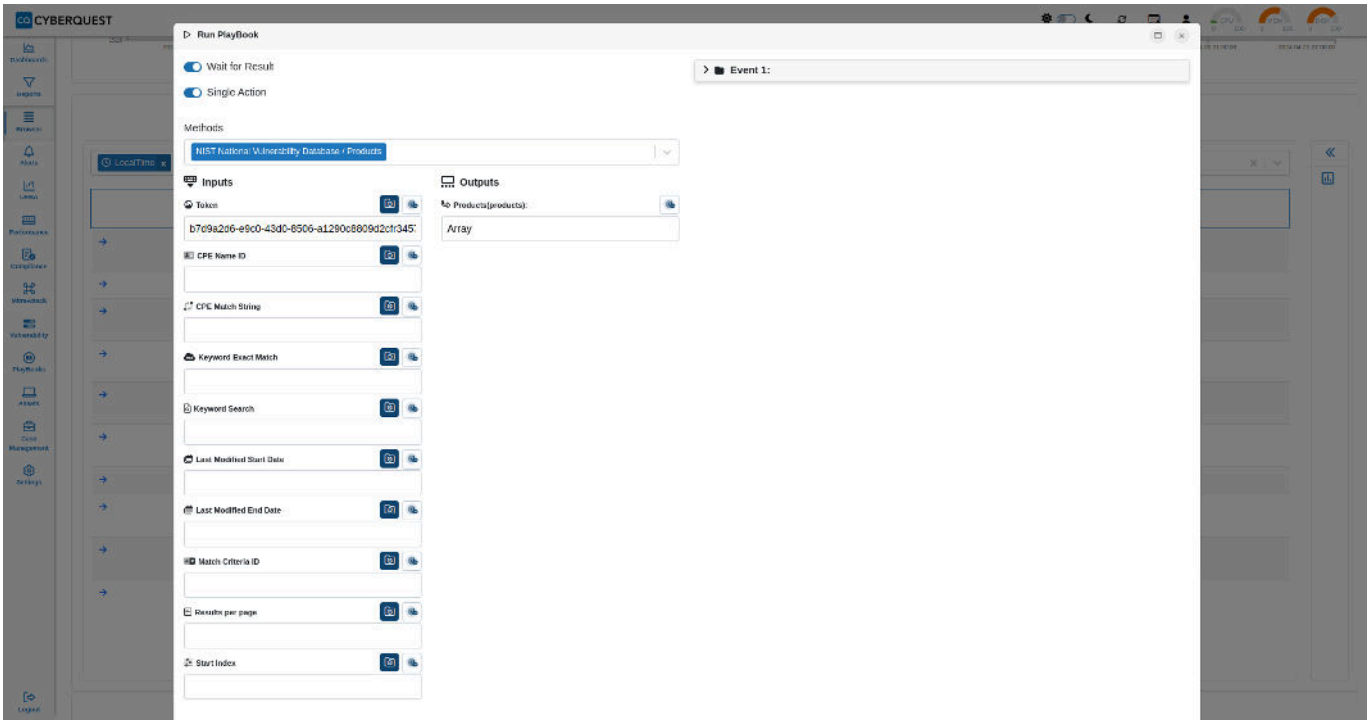


Inputs	Description
Token (is required)	To use the NIST National Vulnerability Database API, you must have an API key.
Change Start Date	These parameters(Change Start Date and Change End Date) return any CVE that changed during the specified period. Please note, this is different from the last modified date parameters used with other APIs. If filtering by the change date, both Change Start Date and Change End Date are REQUIRED. The maximum allowable range when using any date range parameters is 120 consecutive days
Change End Date	These parameters(Change Start Date and Change End Date) return any CVE that changed during the specified period. Please note, this is different from the last modified date parameters used with other APIs. If filtering by the change date, both Change Start Date and Change End Date are REQUIRED. The maximum allowable range when using any date range parameters is 120 consecutive days
CVE ID	This parameter returns the complete change history for a specific vulnerability identified by its unique Common Vulnerabilities and Exposures identifier (the CVE ID)
Event Name	This parameter returns all CVE associated with a specific type of change event.
Results per page	This parameter specifies the maximum number of change events to be returned in a single API response. For network considerations, the default value and maximum allowable limit is 5,000
Start Index	This parameter specifies the index of the first change events to be returned in the response data. The index is zero-based, meaning the first change events is at index zero

Outputs	Description
CVE Changes (cveChanges)	The CVE Changes object contains an array of objects equal to the number of change events returned in the response

NIST National Vulnerability Database/Products method

The CPE API is used to easily retrieve information on a single CPE record or a collection of CPE records from the Official CPE Dictionary.

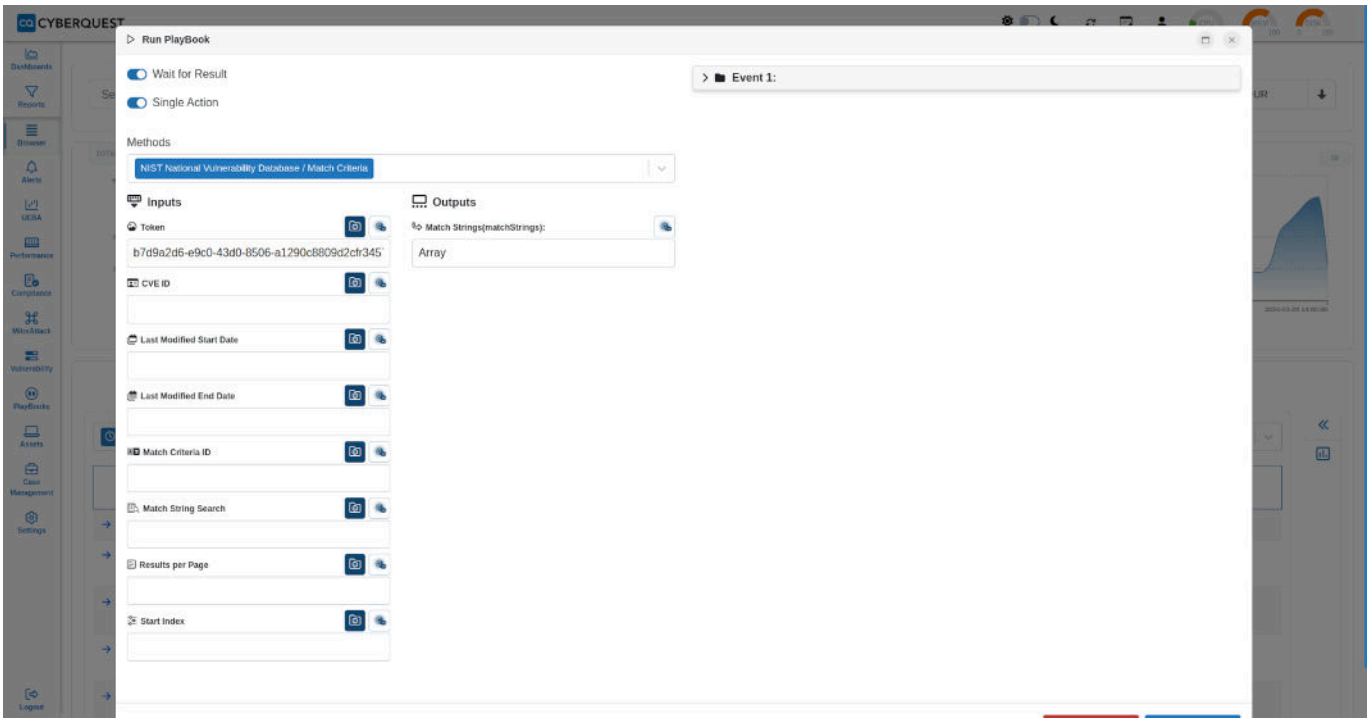


Inputs	Description
Token (is required)	To use the NIST National Vulnerability Database API, you must have an API key.
CPE Name ID	This parameter returns a specific CPE record identified by a Universal Unique Identifier (UUID)
CPE Match String	This parameter returns CPE Names that exist in the Official CPE Dictionary
Keyword Exact Match	By default, this parameter returns any CVE where a word or phrase is found in the current description
Keyword Search	This parameter returns only the CVEs where a word or phrase is found in the current description.
Last Modified Start Date	These parameters (Last Modified Start Date and Last Modified End Date) return only the source records that were last modified during the specified period. If a source record has been modified more recently than the specified period, it will not be included in the response. If filtering by the last modified date, both Last Modified Start Date and Last Modified End Date are REQUIRED. The maximum allowable range when using any date range parameters is 120 consecutive days.
Last Modified End Date	These parameters (Last Modified Start Date and Last Modified End Date) return only the source records that were last modified during the specified period. If a source record has been modified more recently than the specified period, it will not be included in the response. If filtering by the last modified date, both Last Modified Start Date and Last Modified End Date are REQUIRED. The maximum allowable range when using any date range parameters is 120 consecutive days.
Match Criteria ID	This parameter returns all CPE records associated with a match string identified by its {uuid}. Match Criteria ID will only accept a properly formatted {uuid}
Results per page	This parameter specifies the maximum number of source records to be returned in a single API response. For network considerations, the default value and maximum allowable limit is 1,000
Start Index	This parameter specifies the index of the first source record to be returned in the response data. The index is zero-based, meaning the first source record is at index zero

Outputs	Description
Products (products)	he products object contains an array of objects equal to the number of records returned in the response and is sorted in ascending order by the created property of the cpe object.

NIST National Vulnerability Database/Match Criteria method

The CPE Match Criteria API is used to easily retrieve the complete list of valid CPE Match Strings. Unlike a CPE Name, match strings and match string ranges do not require a value in the part, vendor, product, or version components.

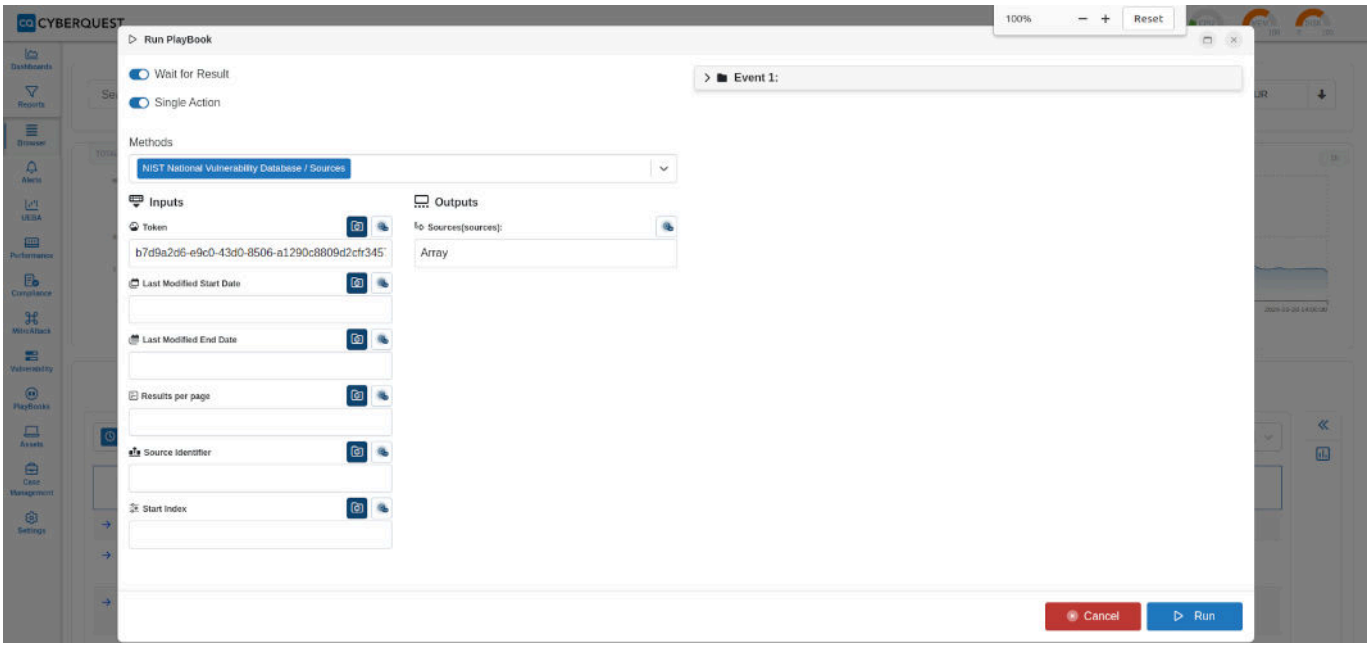


Inputs	Description
Token (is required)	To use the NIST National Vulnerability Database API, you must have an API key.
CVE ID	This parameter returns the complete change history for a specific vulnerability identified by its unique Common Vulnerabilities and Exposures identifier (the CVE ID)
Last Modified Start Date	These parameters (Last Modified Start Date and Last Modified End Date) return only the source records that were last modified during the specified period. If a source record has been modified more recently than the specified period, it will not be included in the response. If filtering by the last modified date, both Last Modified Start Date and Last Modified End Date are REQUIRED. The maximum allowable range when using any date range parameters is 120 consecutive days.
Last Modified End Date	These parameters (Last Modified Start Date and Last Modified End Date) return only the source records that were last modified during the specified period. If a source record has been modified more recently than the specified period, it will not be included in the response. If filtering by the last modified date, both Last Modified Start Date and Last Modified End Date are REQUIRED. The maximum allowable range when using any date range parameters is 120 consecutive days.
Match Criteria ID	This parameter returns all CPE records associated with a match string identified by its {uuid}. Match Criteria ID will only accept a properly formatted {uuid}
Match String Search	This parameter returns all CPE Match Strings that conform to the pattern of the Match String Search
Results per Page	This parameter specifies the maximum number of source records to be returned in a single API response. For network considerations, the default value and maximum allowable limit is 1,000
Start Index	This parameter specifies the index of the first source record to be returned in the response data. The index is zero-based, meaning the first source record is at index zero

Outputs	Description
Match Strings (matchStrings)	The Match Strings object contains an array of objects equal to the number of records returned in the Image Conversion from URLresponse and is sorted in ascending order by the created property of the matchString object

NIST National Vulnerability Database/Sources method

The Source API is used to easily retrieve detailed information on the organizations that provide the data contained in the NVD dataset.



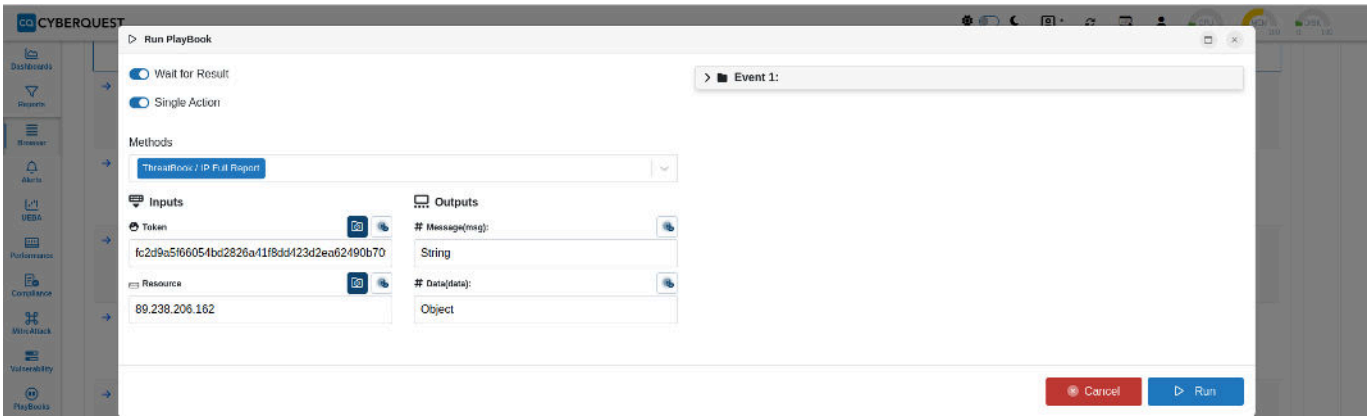
Inputs	Description
Token (is required)	To use the NIST National Vulnerability Database API, you must have an API key.
Last Modified Start Date	These parameters (Last Modified Start Date and Last Modified End Date) return only the source records that were last modified during the specified period. If a source record has been modified more recently than the specified period, it will not be included in the response. If filtering by the last modified date, both Last Modified Start Date and Last Modified End Date are REQUIRED. The maximum allowable range when using any date range parameters is 120 consecutive days.
Last Modified End Date	These parameters (Last Modified Start Date and Last Modified End Date) return only the source records that were last modified during the specified period. If a source record has been modified more recently than the specified period, it will not be included in the response. If filtering by the last modified date, both Last Modified Start Date and Last Modified End Date are REQUIRED. The maximum allowable range when using any date range parameters is 120 consecutive days.
Results per page	This parameter specifies the maximum number of source records to be returned in a single API response. For network considerations, the default value and maximum allowable limit is 1,000
Source Identifier	This parameter returns all source records where the exact value of Source Identifier
Start Index	This parameter specifies the index of the first source record to be returned in the response data. The index is zero-based, meaning the first source record is at index zero

Outputs	Description
Sources (sources)	This object contains the following required data: source name, the email address used by the CVE Program to identify the source, an object containing all email addresses linked to the source, the date and time that the source first appeared in the NVD, and the date and time that the record was last modified

ThreatBook

ThreatBook/IP Full Report method

This endpoint retrieves information about a user, including the privileges and quotas associated to the user.



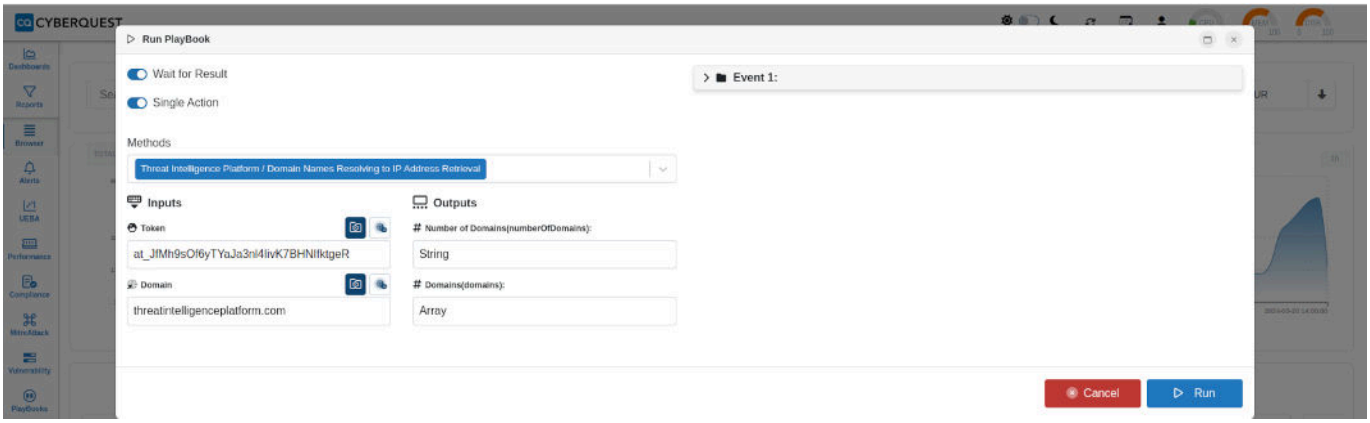
Inputs	Description
Token (is required)	To use the ThreatBook API, you must have an API key.
Resource (is required)	The IP which is investigated

Outputs	Description
Message (msg)	Status of request
Data (data)	The report of the investigated IP from ThreatBook

Threat Intelligence Platform

Threat Intelligence Platform/Domain Names Resolving to IP Address Retrieval method

Retrieve a list of domain names resolving to a given IP address, including subdomains.

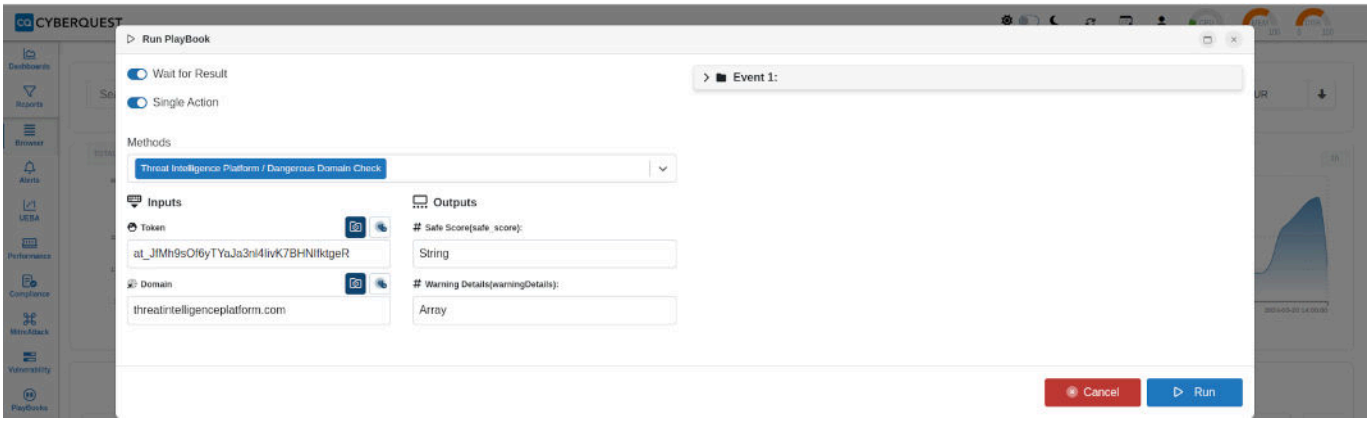


Inputs	Description
Token (is required)	The target domain name.
Domain (is required)	To use the ThreatIntelligence API, you must have an API key.

Outputs	Description
Number of Domains (numberOfDomains)	Number of domain names resolving to a given IP address
Domains (domains)	A list of domain names resolving to a given IP address

Threat Intelligence Platform/Dangerous Domain Check method

For a given domain name, check if it is considered to be dangerous in different security data sources. Dangerous domains could be related to a malware distribution network or host a malicious code.

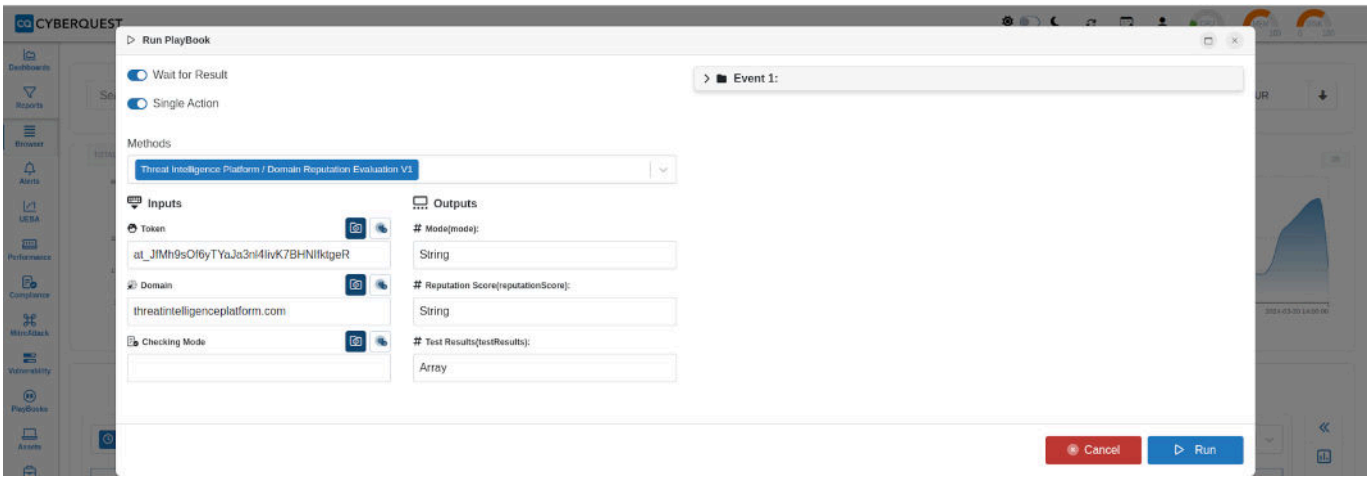


Inputs	Description
Token (is required)	To use the ThreatIntelligence API, you must have an API key.
Domain (is required)	The target domain name

Outputs	Description
Safe Score (safe_score)	Composite safety score based on numerous security data sources. 0 is dangerous, and 100 is safe
Warning Details (warningDetails)	For a dangerous domain, comments regarding why its considered dangerous. Possible warnings:PhishingMalwareSpamBad reputationDenial of service attack

Threat Intelligence Platform/Domain Reputation Evaluation V1 method

Evaluate a domains reputation based on numerous security data sources as well as on an instant hosts audit procedure.

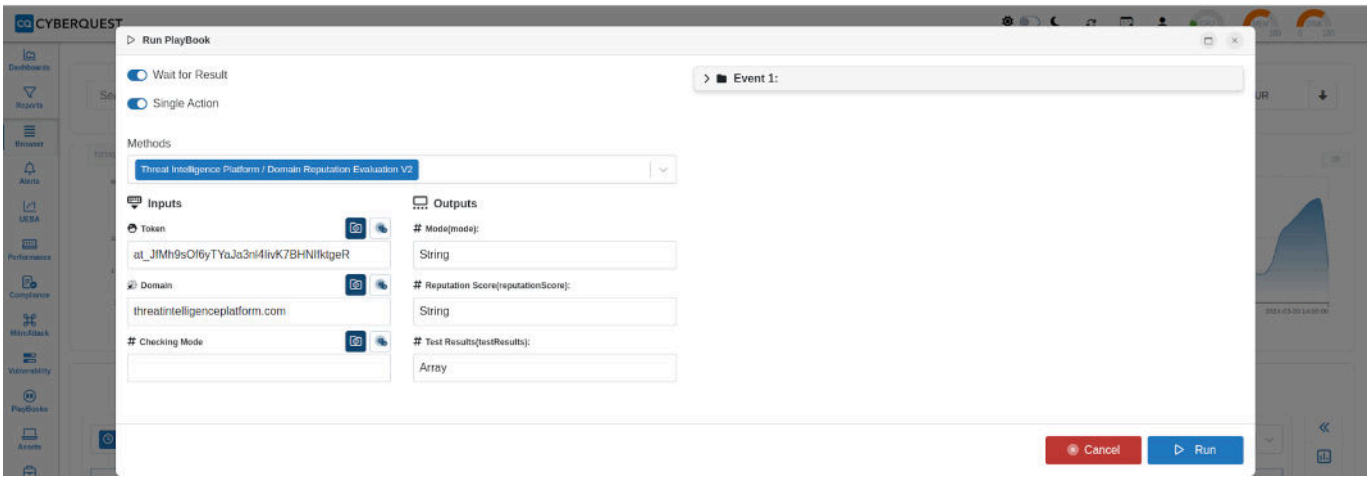


Inputs	Description
Token (is required)	To use the ThreatIntelligence API, you must have an API key.
Domain (is required)	The target domain name or IPv4 address.
Checking Mode	TIP can check the domain specified in two modes:fast (default). Only select test codes will run — i.e., 62 WHOIS Domain status, 82 Malware Databases check, 87 SSL certificate validity, and 93 WHOIS Domain check—while other tests and data collectors will be disabled.full. All tests will be performed, similar to what the TIP GUI displays.

Outputs	Description
Mode (mode)	Selected mode
Reputation Score (reputationScore)	Composite safety score based on numerous security data sources. 0 is dangerous, and 100 is safe
Test Results (testResults)	A list of tests performed on the IP

Threat Intelligence Platform/Domain Reputation Evaluation V2 method

Evaluate a domains reputation based on numerous security data sources as well as on an instant hosts audit procedure.

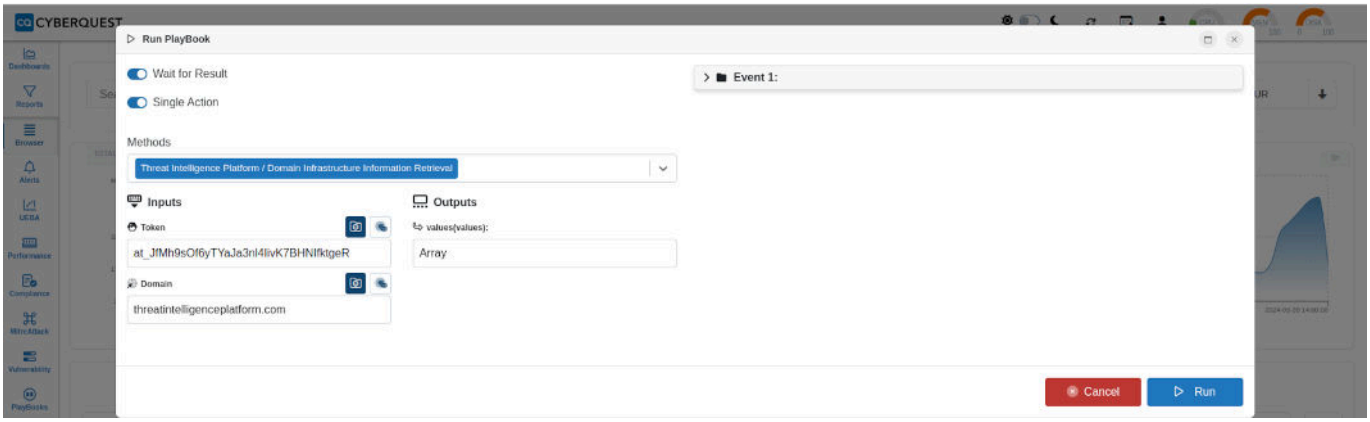


Inputs	Description
Token (is required)	To use the ThreatIntelligence API, you must have an API key.
Domain (is required)	The target domain name or IPv4 address.
Checking Mode	TIP can check the domain specified in two modes:fast (default). Only select test codes will run — i.e., 62 WHOIS Domain status, 82 Malware Databases check, 87 SSL certificate validity, and 93 WHOIS Domain check—while other tests and data collectors will be disabled.full. All tests will be performed, similar to what the TIP GUI displays.

Outputs	Description
Mode (mode)	Selected mode
Reputation Score (reputationScore)	Composite safety score based on numerous security data sources. 0 is dangerous, and 100 is safe.
Test Results (testResults)	A list of tests performed on the IP

Threat Intelligence Platform/Domain Infrastructure Information Retrieval method

Get a list of web, mail, and name servers for a particular domain name. Determine the IP address, geolocation, and subnetwork information for each infrastructure entry.

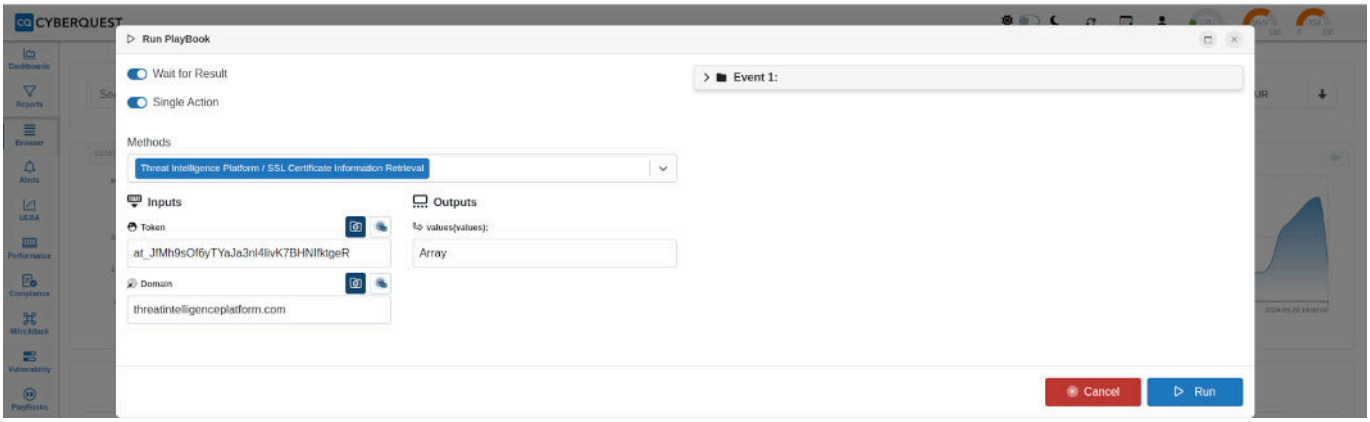


Inputs	Description
Token (is required)	To use the ThreatIntelligence API, you must have an API key.
Domain (is required)	The target domain name.

Outputs	Description
values (values)	The results of the API call

Threat Intelligence Platform/SSL Certificate Information Retrieval method

For a given domain name, get detailed information about its SSL Certificate and the complete SSL Certificate chain.

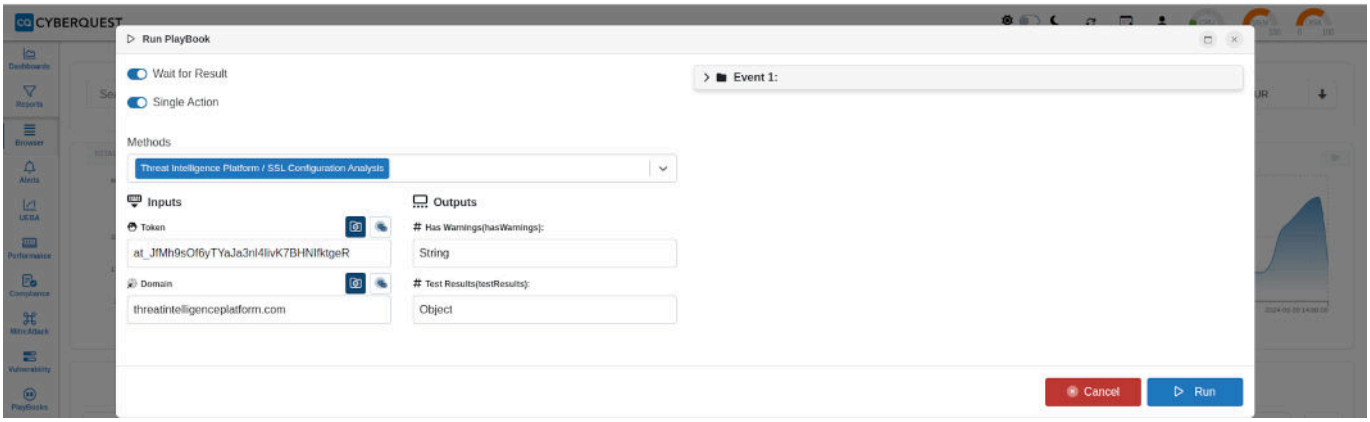


Inputs	Description
Token (is required)	To use the ThreatIntelligence API, you must have an API key.
Domain (is required)	The target domain name.

Outputs	Description
values (values)	The results of the API call

Threat Intelligence Platform/SSL Configuration Analysis method

For a given domain name, establish and test SSL connection to the host and analyze how it is configured - to detect common configuration issues potentially leading to vulnerabilities.



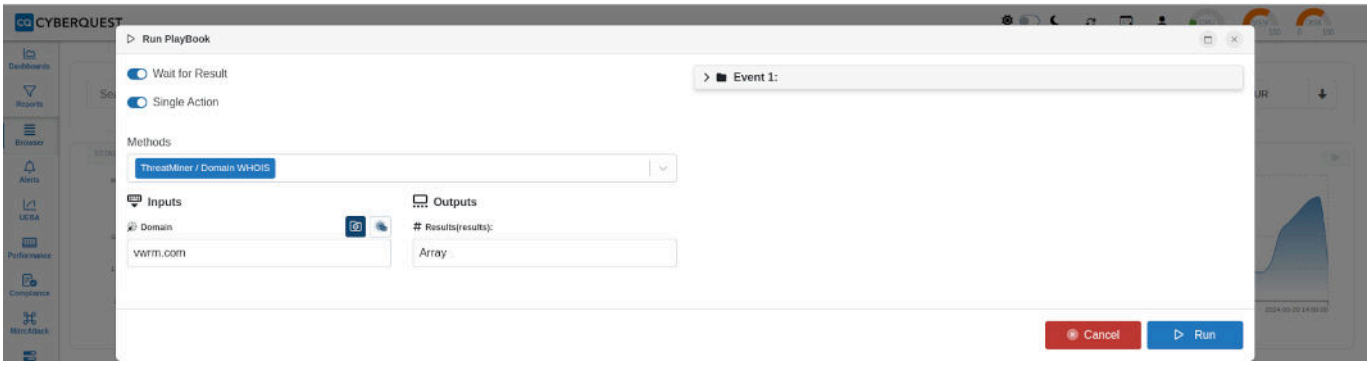
Inputs	Description
Token (is required)	To use the ThreatIntelligence API, you must have an API key
Domain (is required)	The target domain name

Outputs	Description
Has Warnings (hasWarnings)	If true - there are some warnings for the target host
Test Results (testResults)	A list of tests with details

ThreatMiner

ThreatMiner/Domain WHOIS method

Based on the query, this function returns threat analysis details for the provided domain.

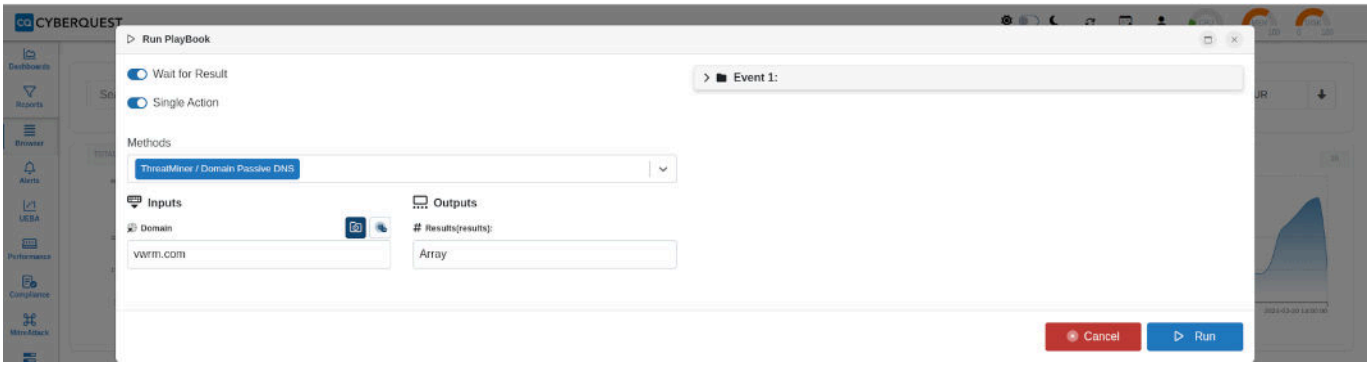


Inputs	Description
Domain (is required)	The Domain which is examined

Outputs	Description
Results (results)	The results of the API call

ThreatMiner/Domain Passive DNS method

Based on the query, this function returns threat analysis details for the provided domain.

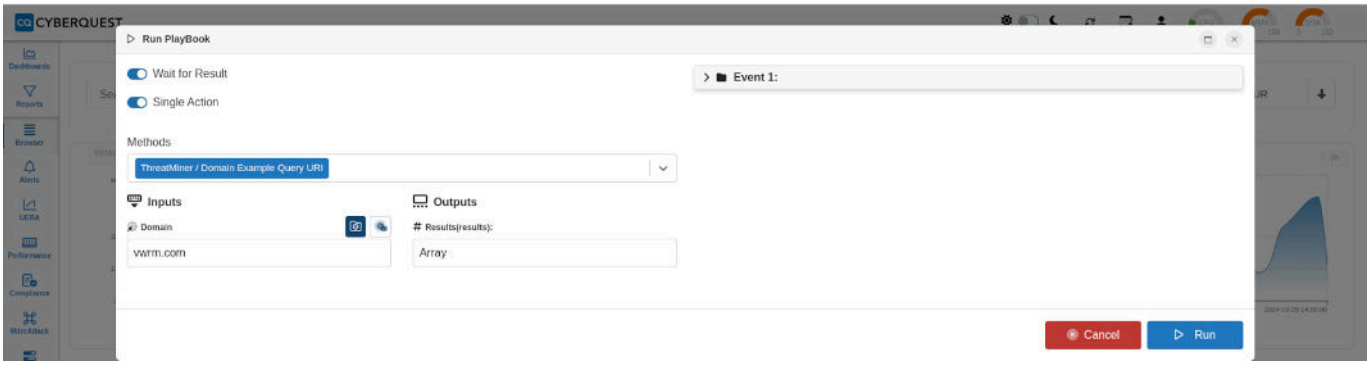


Inputs	Description
Domain (is required)	The Domain which is examined

Outputs	Description
Results (results)	The results of the API call

ThreatMiner/Domain Example Query URI method

Based on the query, this function returns threat analysis details for the provided domain.

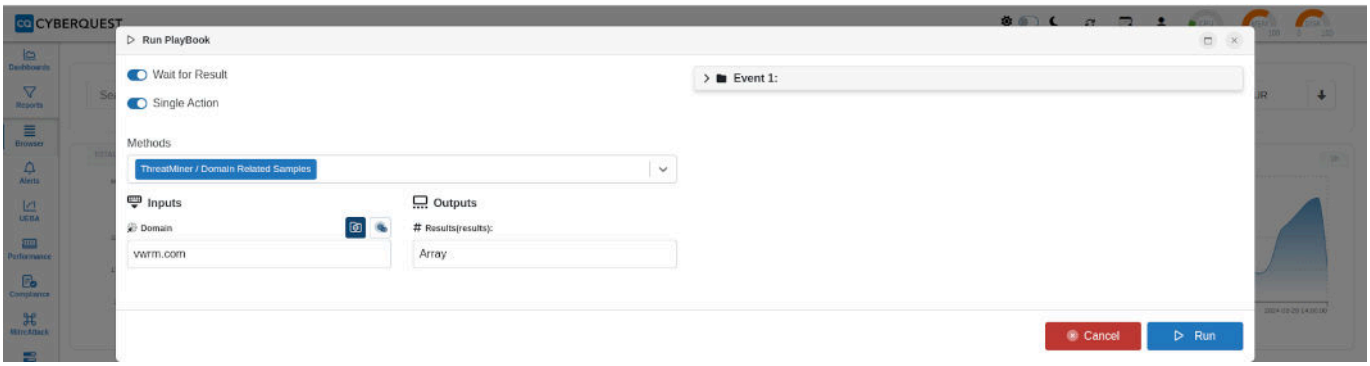


Inputs	Description
Domain (is required)	The Domain which is examined

Outputs	Description
Results (results)	The results of the API call

ThreatMiner/Domain Related Samples method

Based on the query, this function returns threat analysis details for the provided domain.

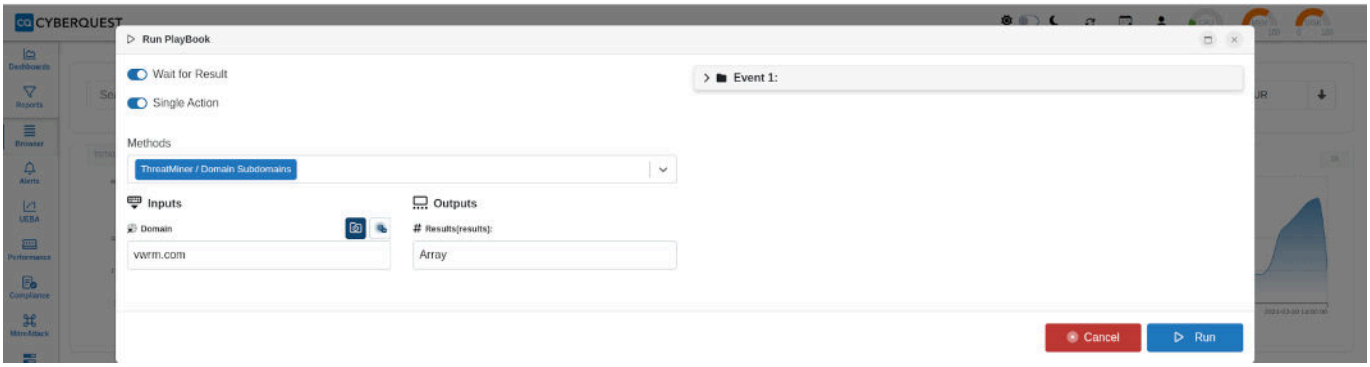


Inputs	Description
Domain (is required)	The Domain which is examined

Outputs	Description
Results (results)	The results of the API call

ThreatMiner/Domain Subdomains method

Based on the query, this function returns threat analysis details for the provided domain.

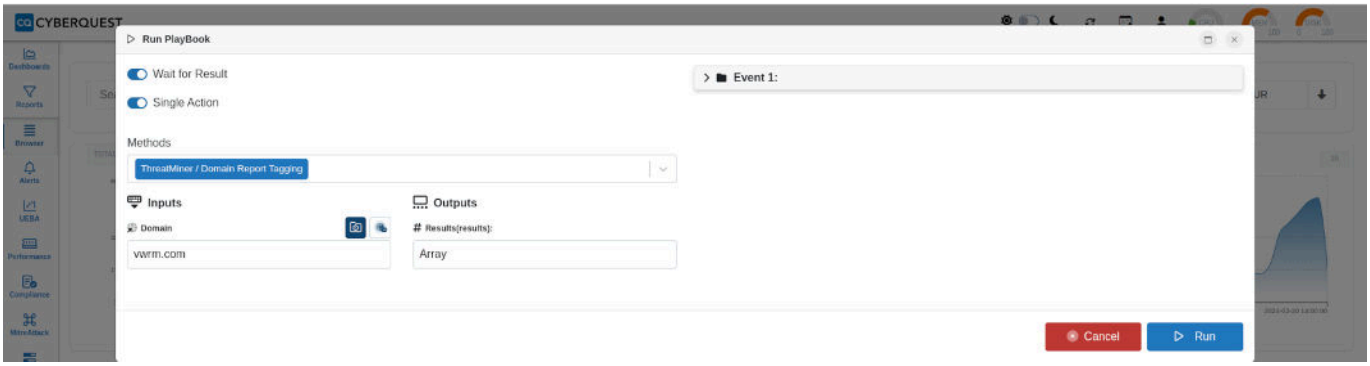


Inputs	Description
Domain (is required)	The Domain which is examined

Outputs	Description
Results (results)	The results of the API call

ThreatMiner/Domain Report Tagging method

Based on the query, this function returns threat analysis details for the provided domain.

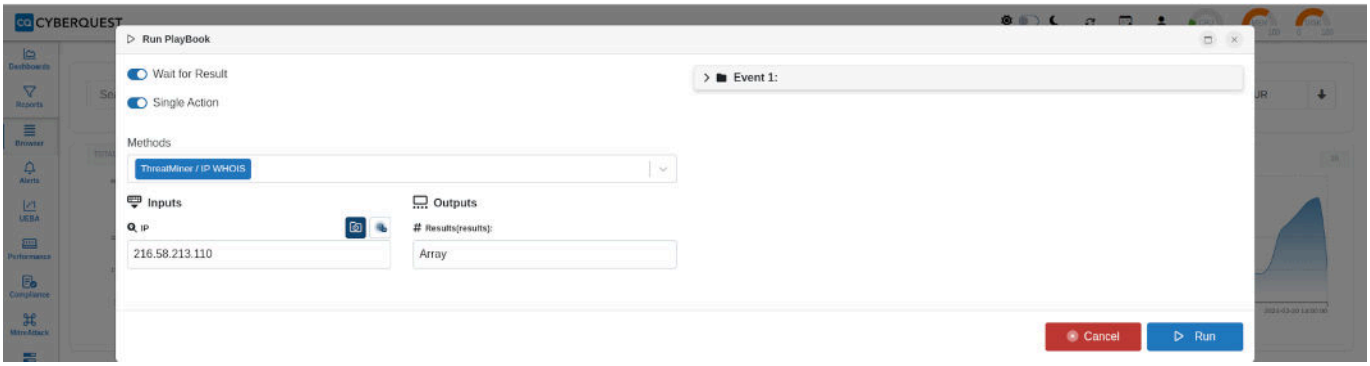


Inputs	Description
Domain (is required)	The Domain which is examined

Outputs	Description
Results (results)	The results of the API call

ThreatMiner/IP WHOIS method

Based on the query, this function returns threat analysis details for the provided ip.

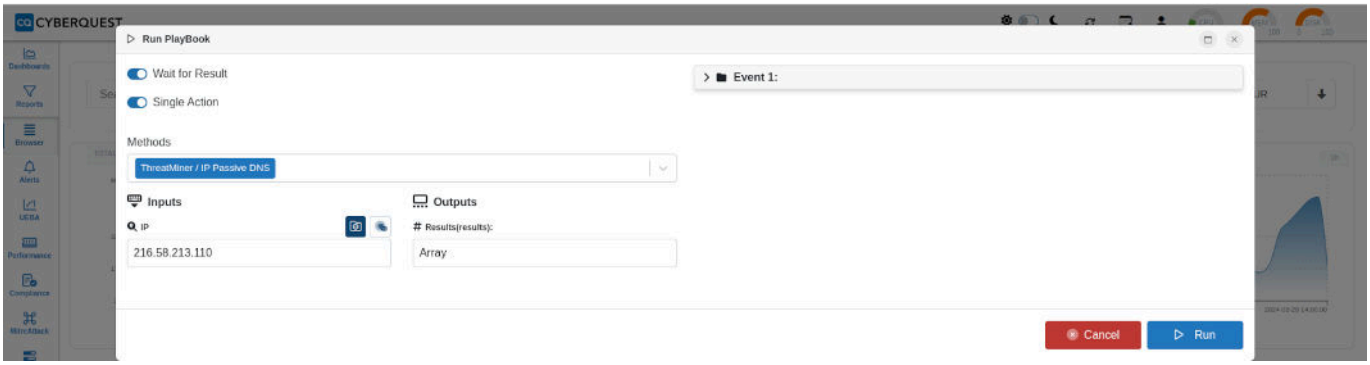


Inputs	Description
IP (is required)	The IP which is examined

Outputs	Description
Results (results)	The results of the API call

ThreatMiner/IP Passive DNS method

Based on the query, this function returns threat analysis details for the provided ip.

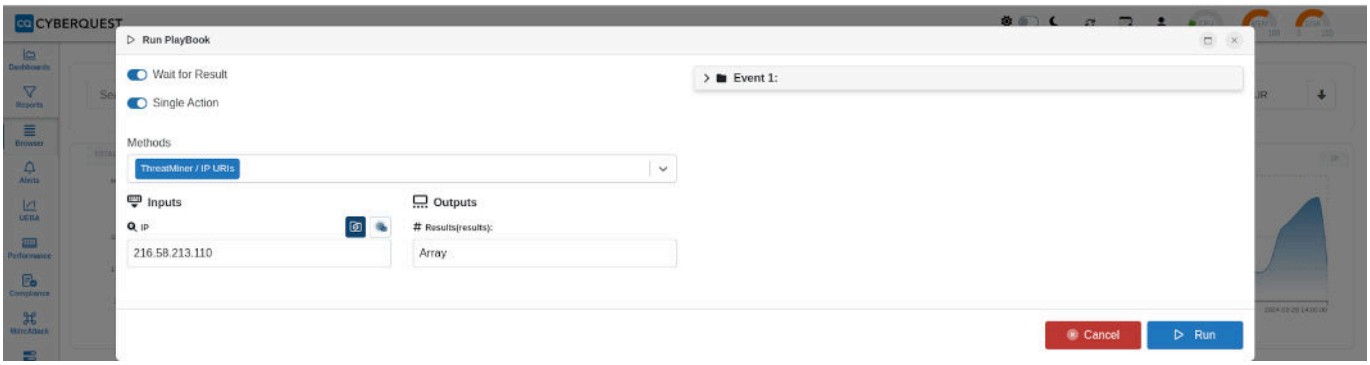


Inputs	Description
IP (is required)	The IP which is examined

Outputs	Description
Results (results)	The results of the API call

ThreatMiner/IP URIs method

Based on the query, this function returns threat analysis details for the provided ip.

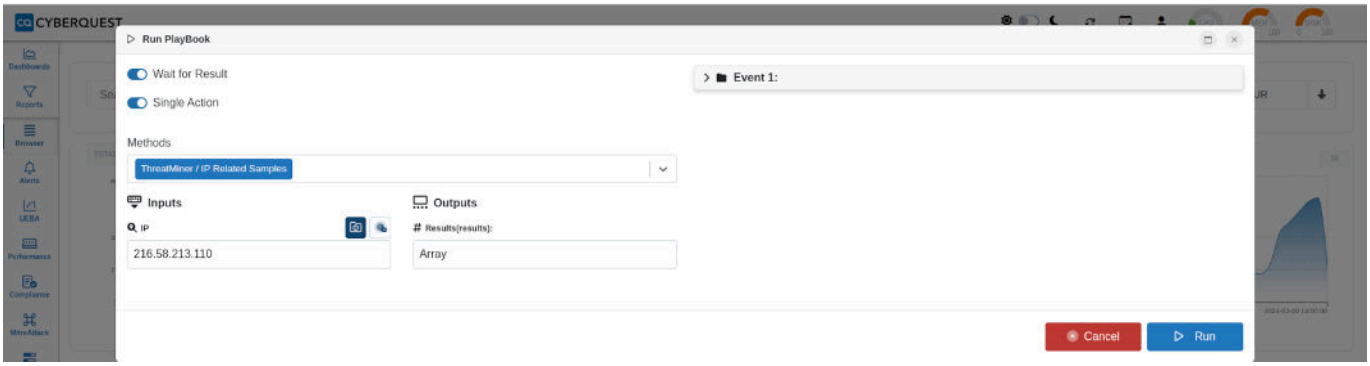


Inputs	Description
IP (is required)	The IP which is examined

Outputs	Description
Results (results)	The results of the API call

ThreatMiner/IP Related Samples method

Based on the query, this function returns threat analysis details for the provided ip.

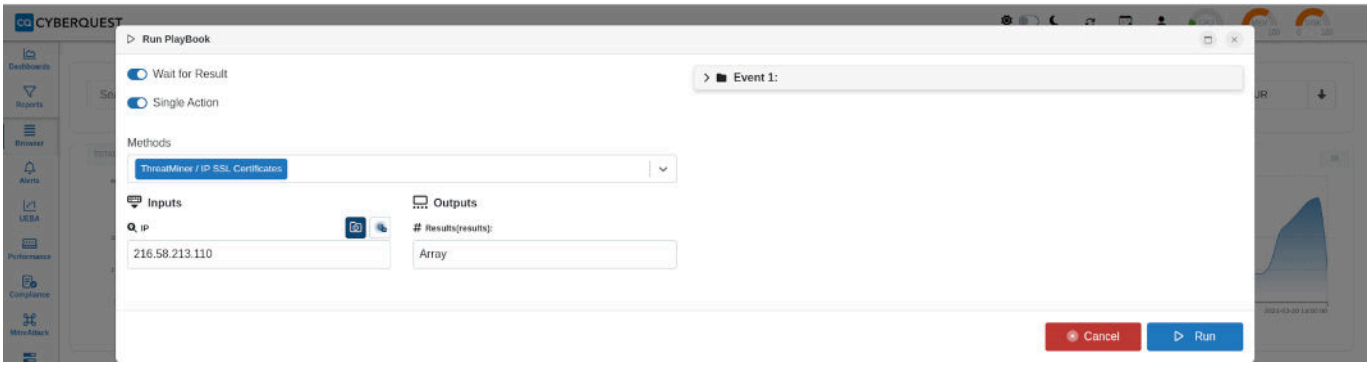


Inputs	Description
IP (is required)	The IP which is examined

Outputs	Description
Results (results)	The results of the API call

ThreatMiner/IP SSL Certificates method

Based on the query, this function returns threat analysis details for the provided ip.

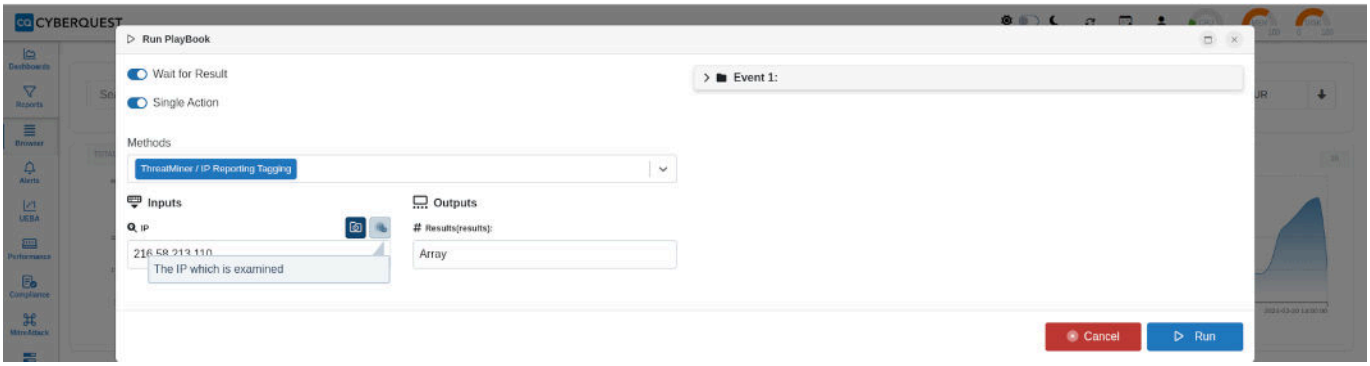


Inputs	Description
IP (is required)	The IP which is examined

Outputs	Description
Results (results)	The results of the API call

ThreatMiner/IP Reporting Tagging method

Based on the query, this function returns threat analysis details for the provided ip.

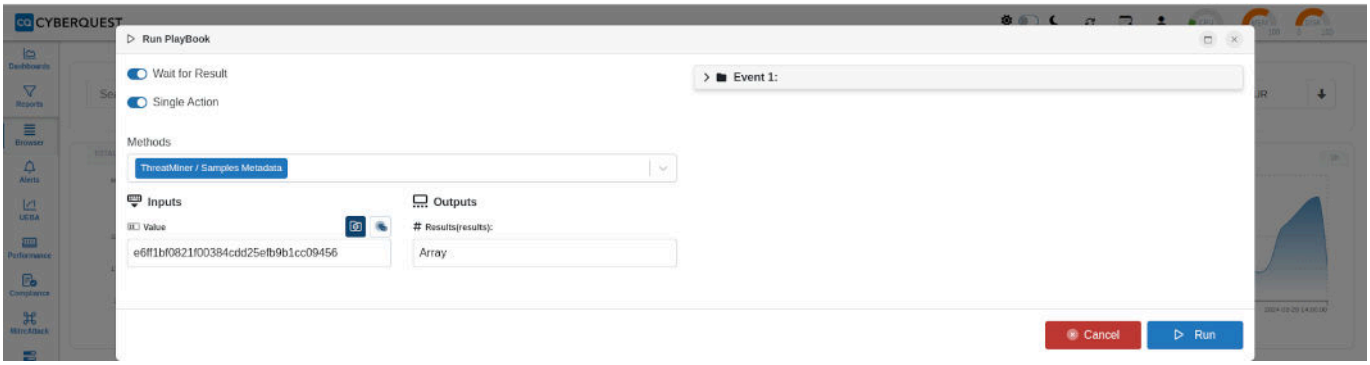


Inputs	Description
IP (is required)	The IP which is examined

Outputs	Description
Results (results)	The results of the API call

ThreatMiner/Samples Metadata method

Samples for different query type.

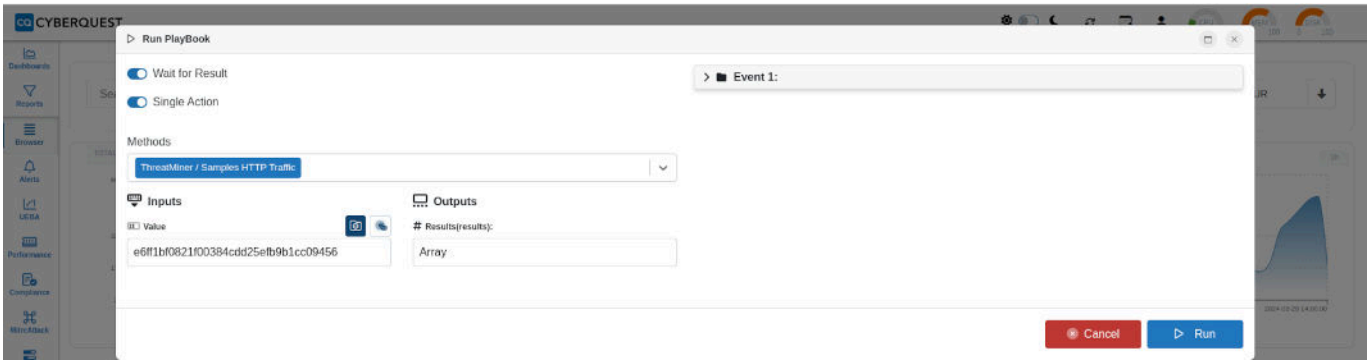


Inputs	Description
Value (is required)	The value which is used to return a Sample

Outputs	Description
Results (results)	The results of the API call

ThreatMiner/Samples HTTP Traffic method

Samples for different query type.

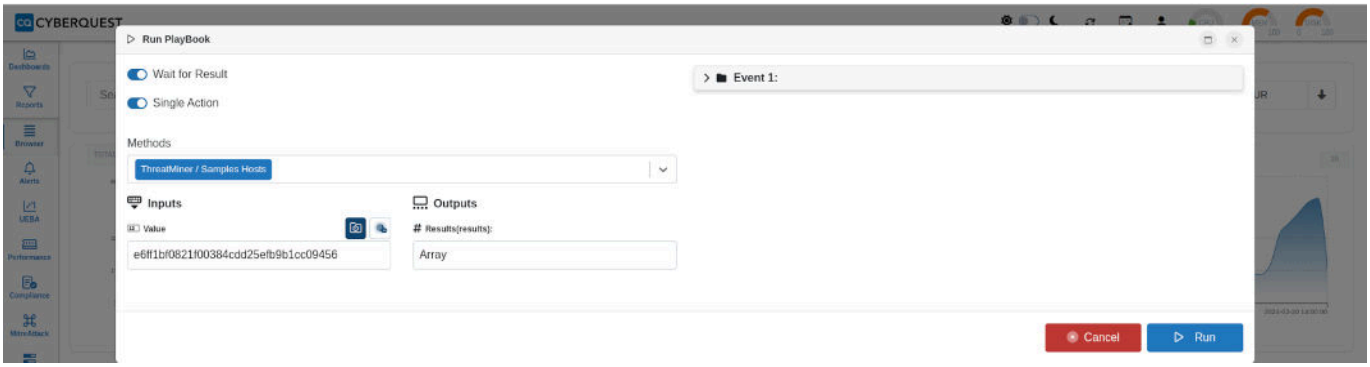


Inputs	Description
Value (is required)	The value which is used to return a Sample

Outputs	Description
Results (results)	The results of the API call

ThreatMiner/Samples Hosts method

Samples for different query type.

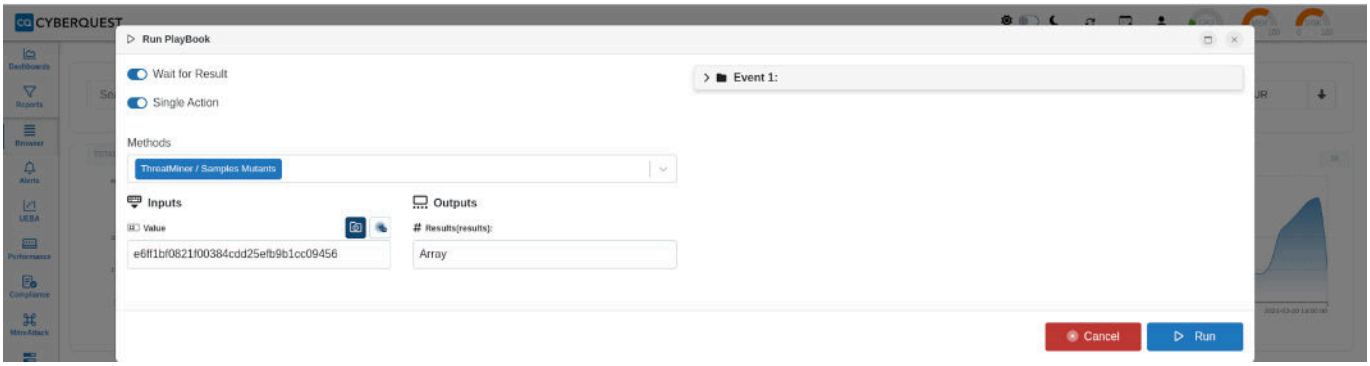


Inputs	Description
Value (is required)	The value which is used to return a Sample

Outputs	Description
Results (results)	The results of the API call

ThreatMiner/Samples Mutants method

Samples for different query type.

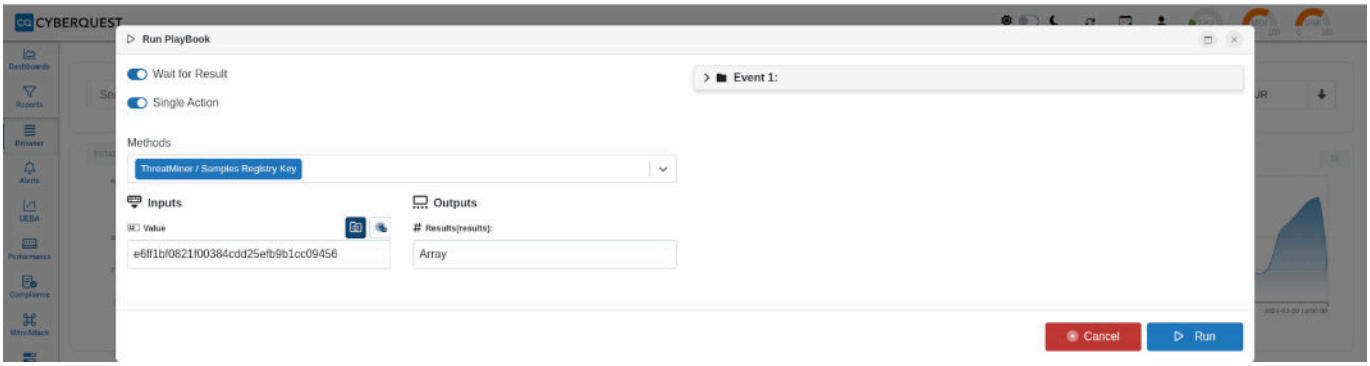


Inputs	Description
Value (is required)	The value which is used to return a Sample

Outputs	Description
Results (results)	The results of the API call

ThreatMiner/Samples Registry Key method

Samples for different query type.

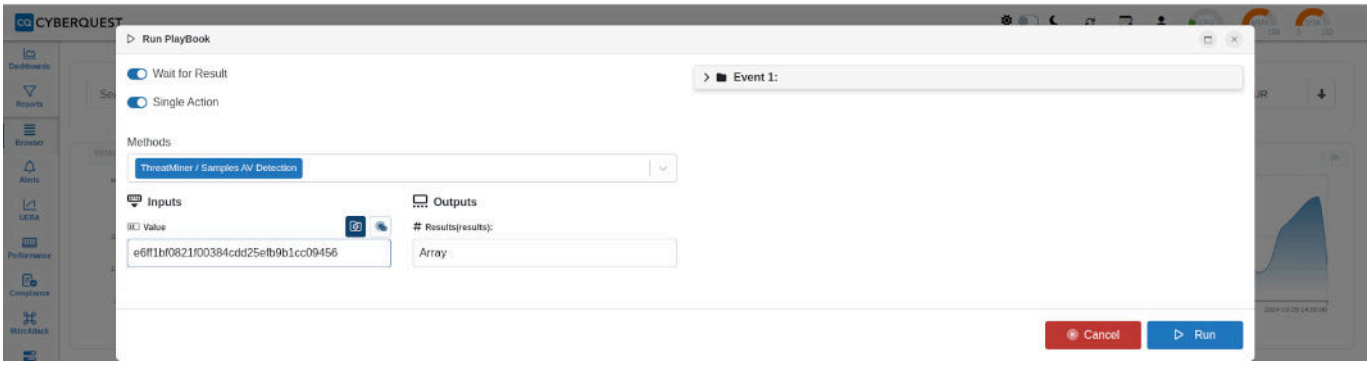


Inputs	Description
Value (is required)	The value which is used to return a Sample

Outputs	Description
Results (results)	The results of the API call

ThreatMiner/Samples AV Detection method

Samples for different query type.

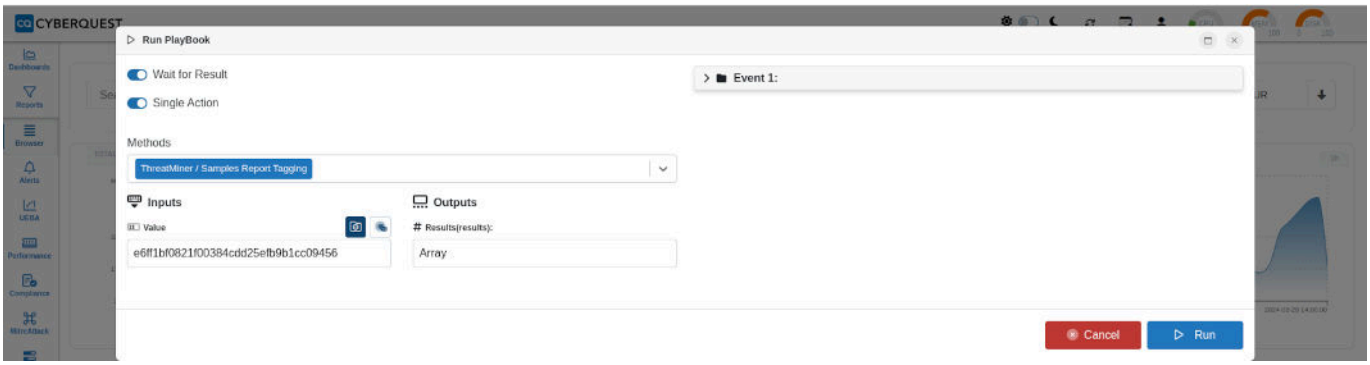


Inputs	Description
Value (is required)	The value which is used to return a Sample

Outputs	Description
Results (results)	The results of the API call

ThreatMiner/Samples Report Tagging method

Samples for different query type.

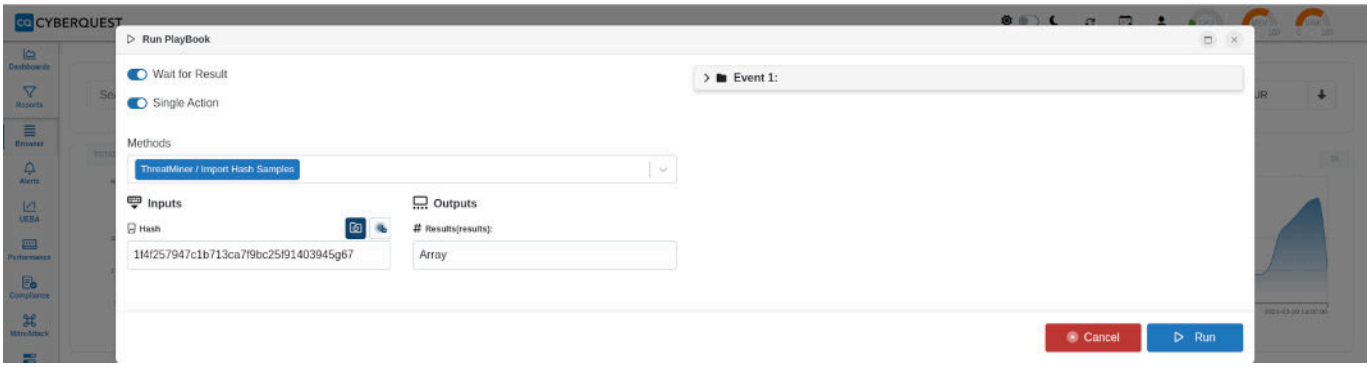


Inputs	Description
Value (is required)	The value which is used to return a Sample

Outputs	Description
Results (results)	The results of the API call

ThreatMiner/Import Hash Samples method

Retrieves the data that detect the level of similarity between two files at the binary level.

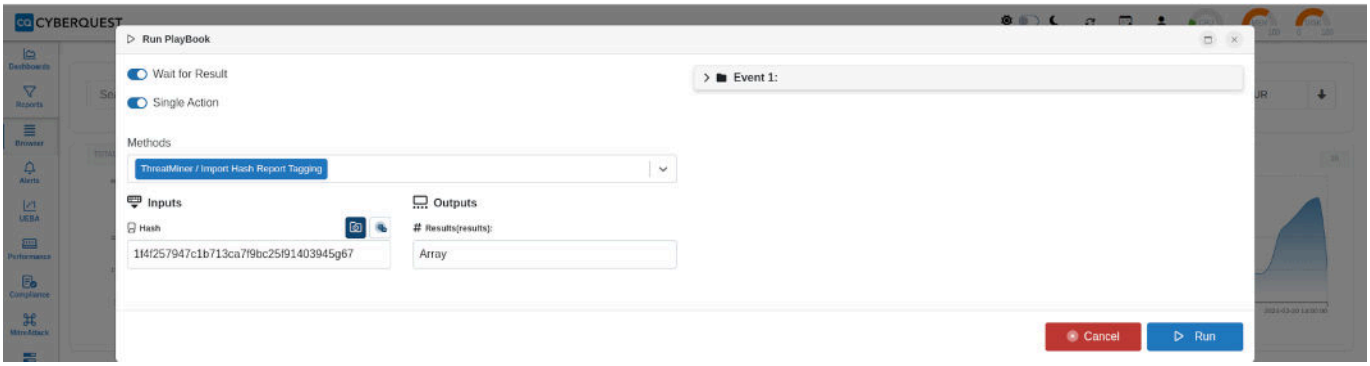


Inputs	Description
Hash (is required)	To get samples query type malware analysis report, it needs an import hash value.

Outputs	Description
Results (results)	The results of the API call

ThreatMiner/Import Hash Report Tagging method

Retrieves the data that detect the level of similarity between two files at the binary level.

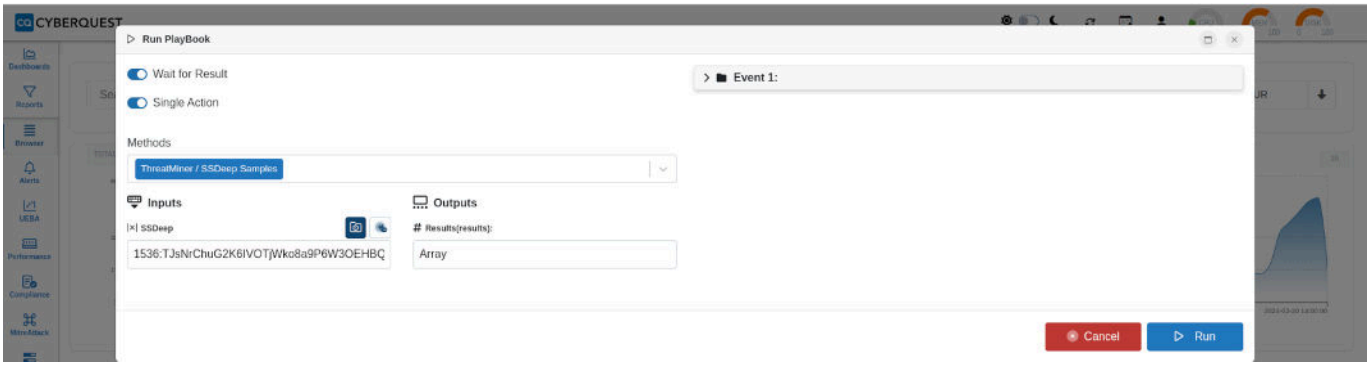


Inputs	Description
Hash (is required)	To get samples query type malware analysis report, it needs an import hash value.

Outputs	Description
Results (results)	The results of the API call

ThreatMiner/SSDeep Samples method

The Binary File Similarity API allows you to retrieve data that measures the degree of similarity between two files at the binary level. This feature provides information on the level of similarity between the contents of the files, helping to identify any resemblances or commonalities between them.

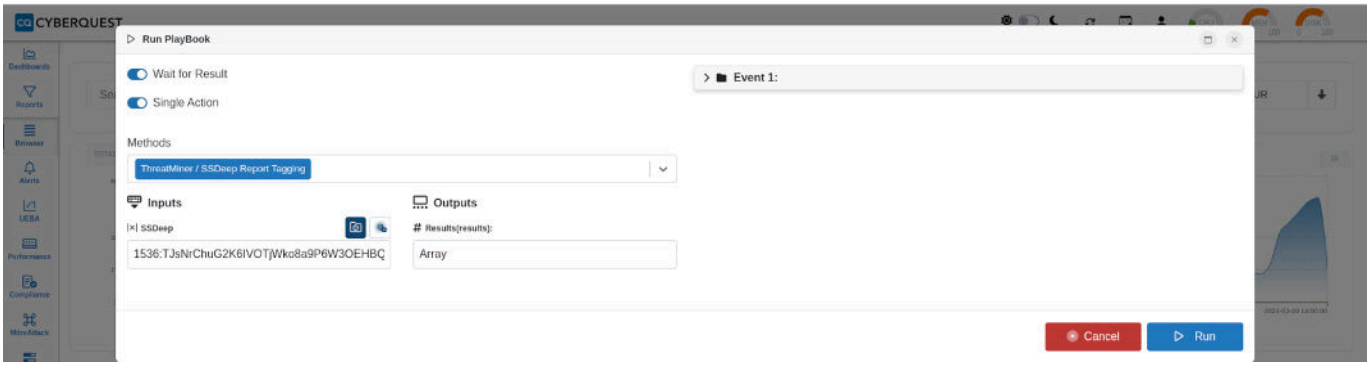


Inputs	Description
SSDeep (is required)	Give the SSDeep hash value, which tries to gauge the degree of binary similarity between two files. Samples query type is the default.

Outputs	Description
Results (results)	The results of the API call

ThreatMiner/SSDeep Report Tagging method

The Binary File Similarity API allows you to retrieve data that measures the degree of similarity between two files at the binary level. This feature provides information on the level of similarity between the contents of the files, helping to identify any resemblances or commonalities between them.

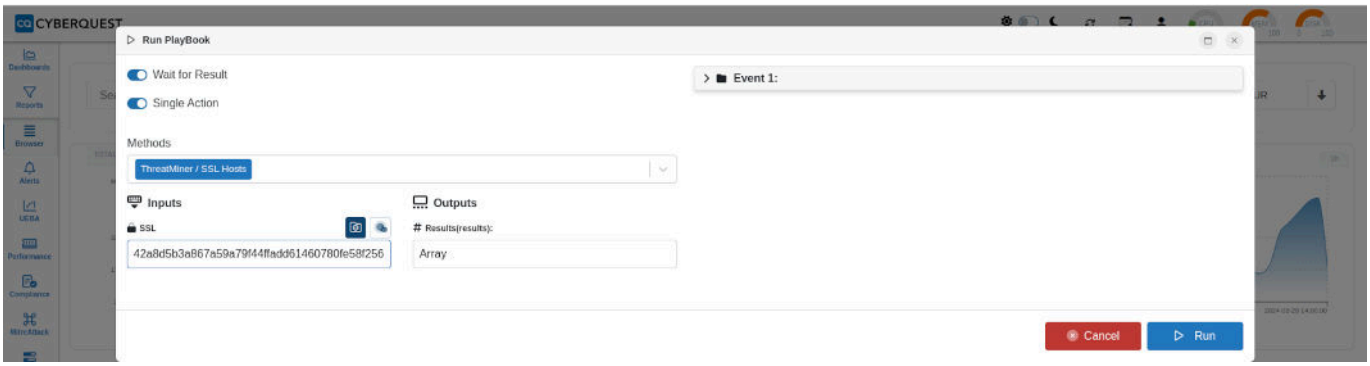


Inputs	Description
SSDeep (is required)	Give the SSDeep hash value, which tries to gauge the degree of binary similarity between two files. Samples query type is the default.

Outputs	Description
Results (results)	The results of the API call

ThreatMiner/SSL Hosts method

Based on the query, this function returns hosts or report tagging.

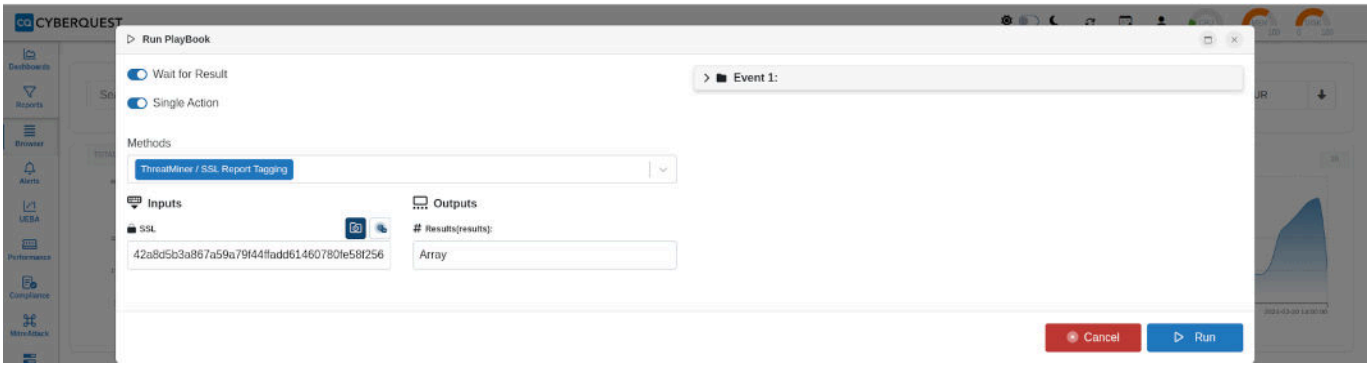


Inputs	Description
SSL (is required)	The SSL value which is examined

Outputs	Description
Results (results)	The results of the API call

ThreatMiner/SSL Report Tagging method

Based on the query, this function returns hosts or report tagging.

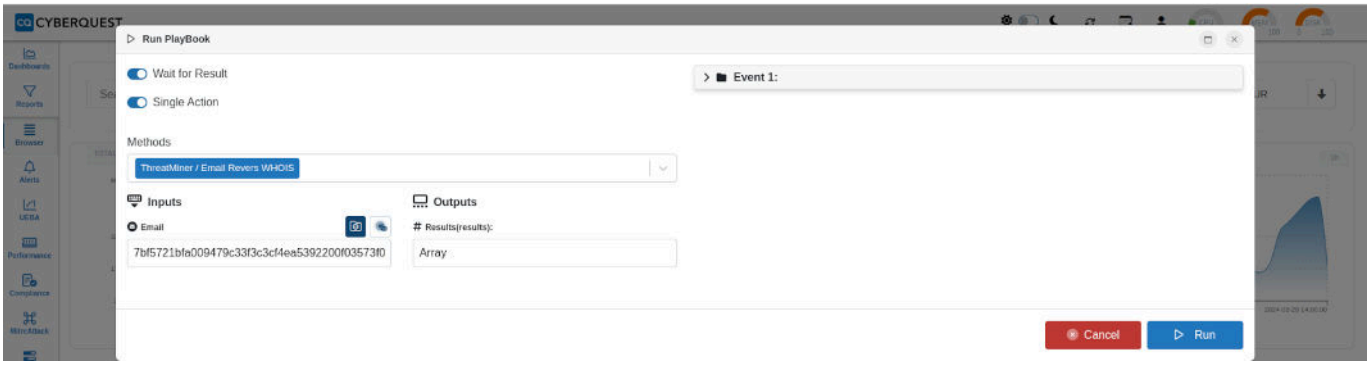


Inputs	Description
SSL (is required)	The SSL value which is examined

Outputs	Description
Results (results)	The results of the API call

ThreatMiner/Email Revers WHOIS method

The Email (Reverse WHOIS) functionality enables you to perform domain searches based on the name, address, telephone number, email address, or physical address of the Registrant as listed in both current and historical Whois records. This feature provides a convenient way to retrieve domain information by utilizing various search criteria associated with the Registrants details.

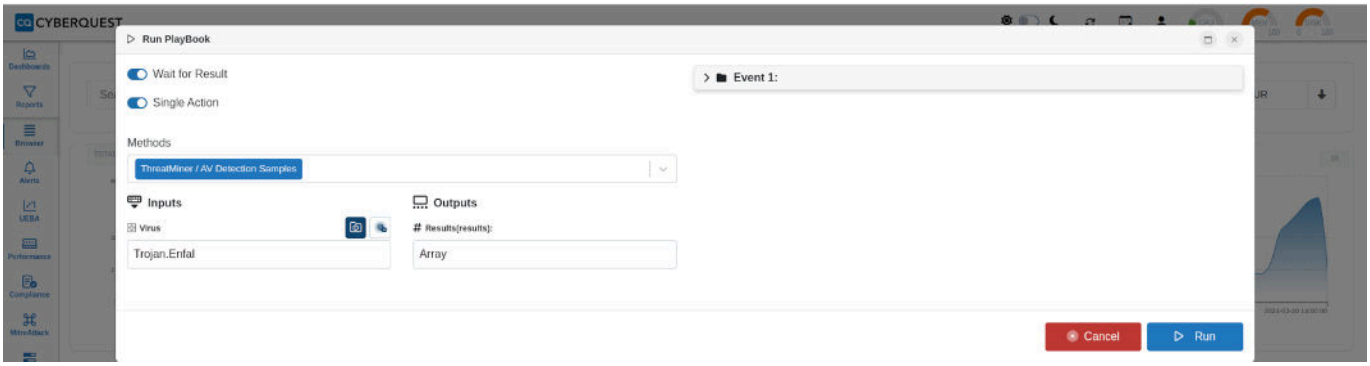


Inputs	Description
Email (is required)	The Email which is examined

Outputs	Description
Results (results)	The results of the API call

ThreatMiner/AV Detection Samples method

Based on query, this function return Report tagging or samples.

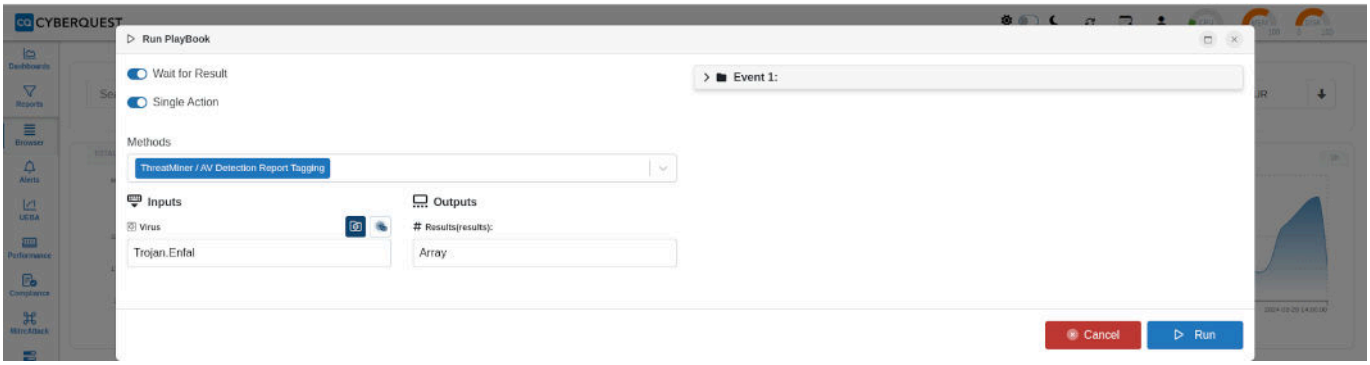


Inputs	Description
Virus (is required)	The type of the virus

Outputs	Description
Results (results)	The results of the API call

ThreatMiner/AV Detection Report Tagging method

Based on query, this function return Report tagging or samples.

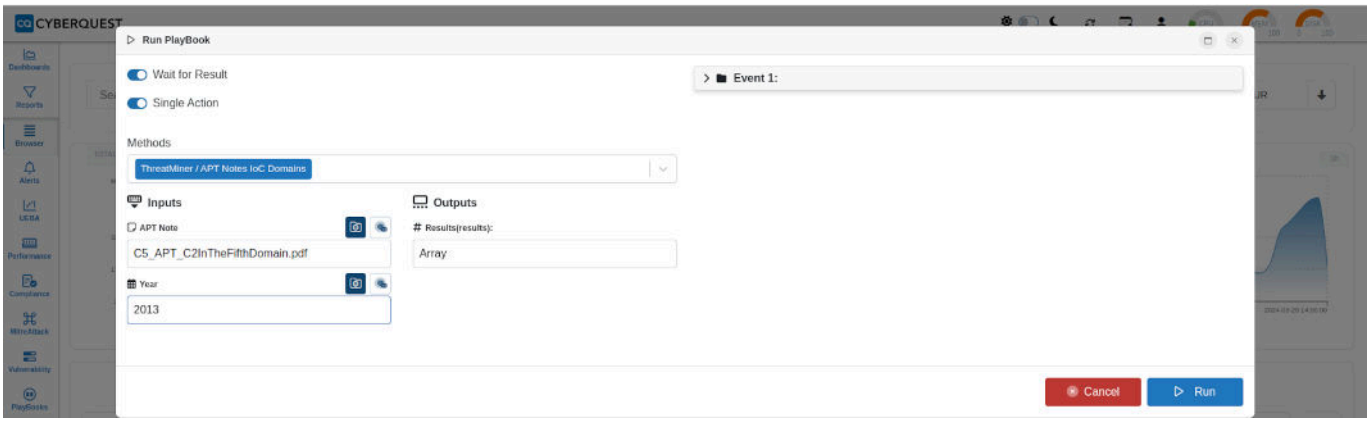


Inputs	Description
Virus (is required)	The type of the virus

Outputs	Description
Results (results)	The results of the API call

ThreatMiner/APT Notes IoC Domains method

Based on query, receive different notes.

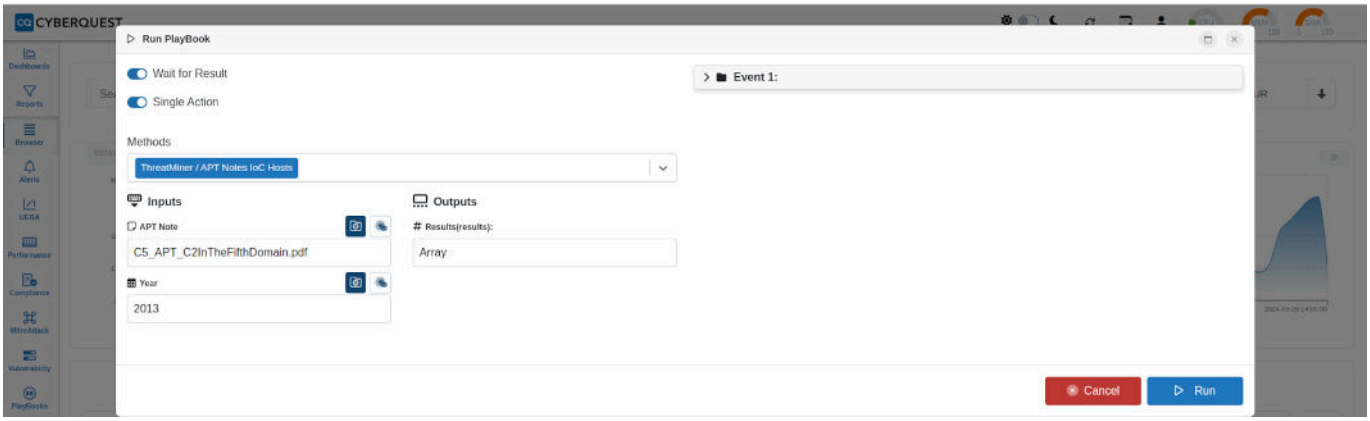


Inputs	Description
APT Note (is required)	The APT Note which is used
Year (is required)	Year

Outputs	Description
Results (results)	The results of the API call

ThreatMiner/APT Notes IoC Hosts method

Based on query, receive different notes.

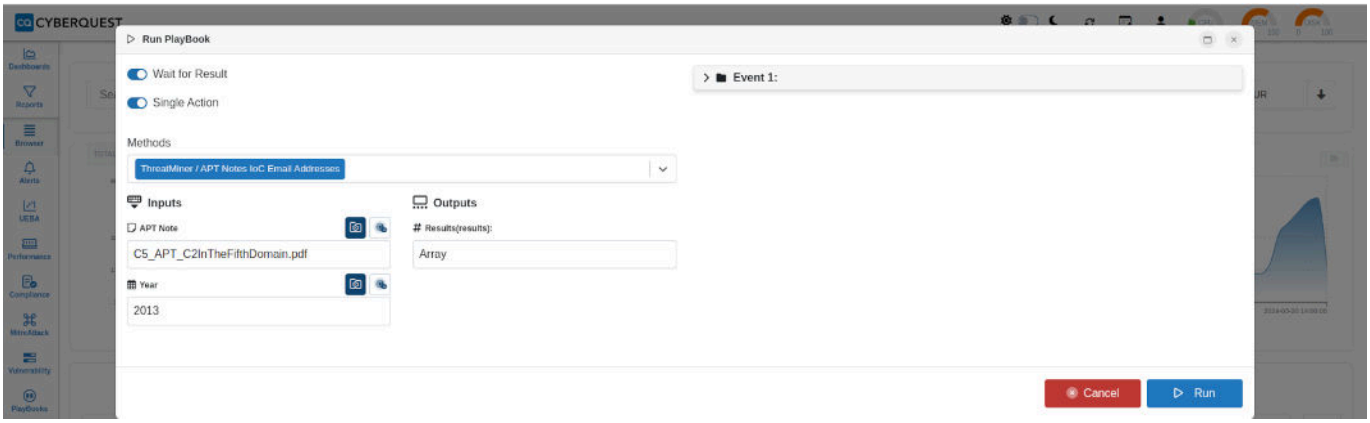


Inputs	Description
APT Note (is required)	The APT Note which is used
Year (is required)	Year

Outputs	Description
Results (results)	The results of the API call

ThreatMiner/APT Notes IoC Email Addresses method

Based on query, receive different notes.

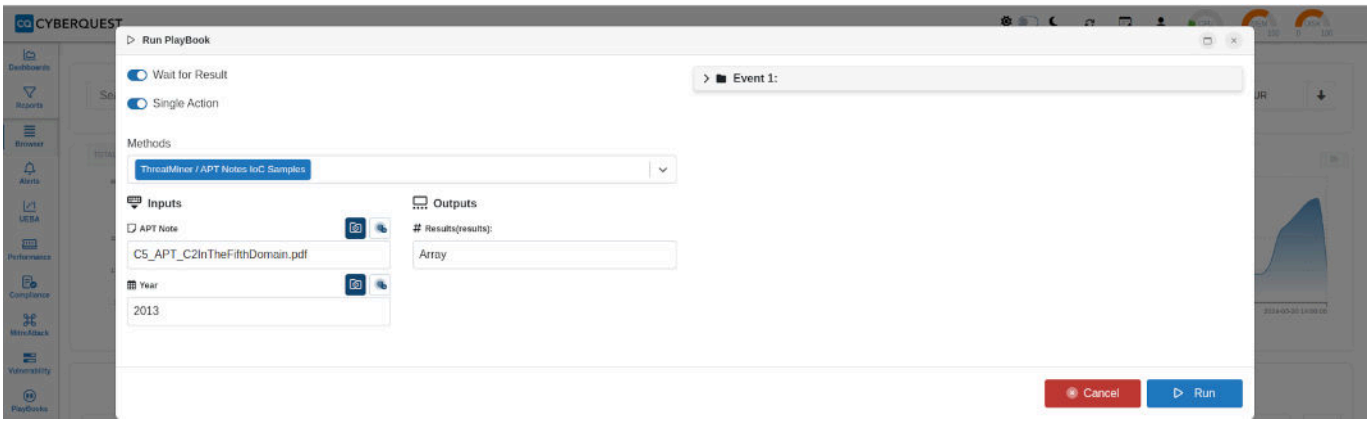


Inputs	Description
APT Note (is required)	The APT Note which is used
Year (is required)	Year

Outputs	Description
Results (results)	The results of the API call

ThreatMiner/APT Notes IoC Samples method

Based on query, receive different reports.

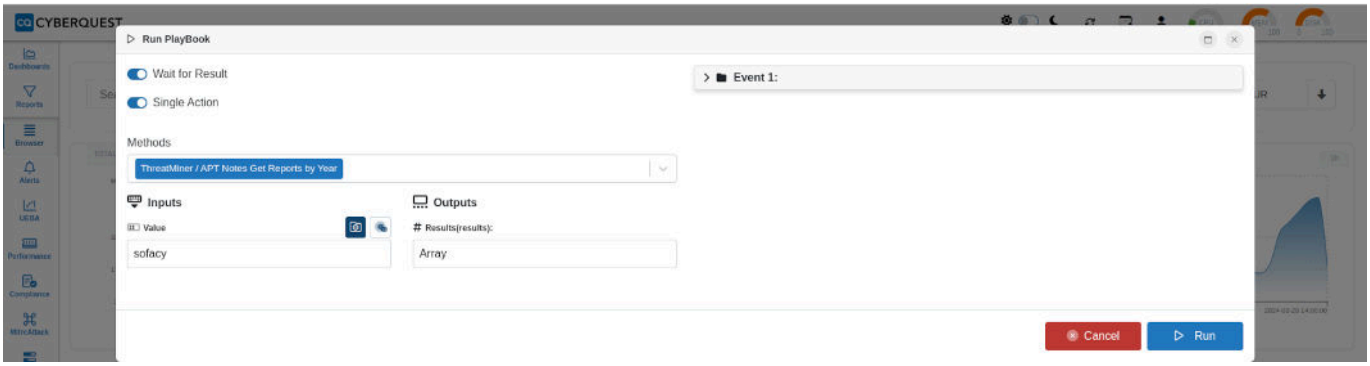


Inputs	Description
APT Note (is required)	The value which is used for this call
Year (is required)	Year

Outputs	Description
Results (results)	The results of the API call

ThreatMiner/APT Notes Get Reports by Year method

Based on query, receive different reports.

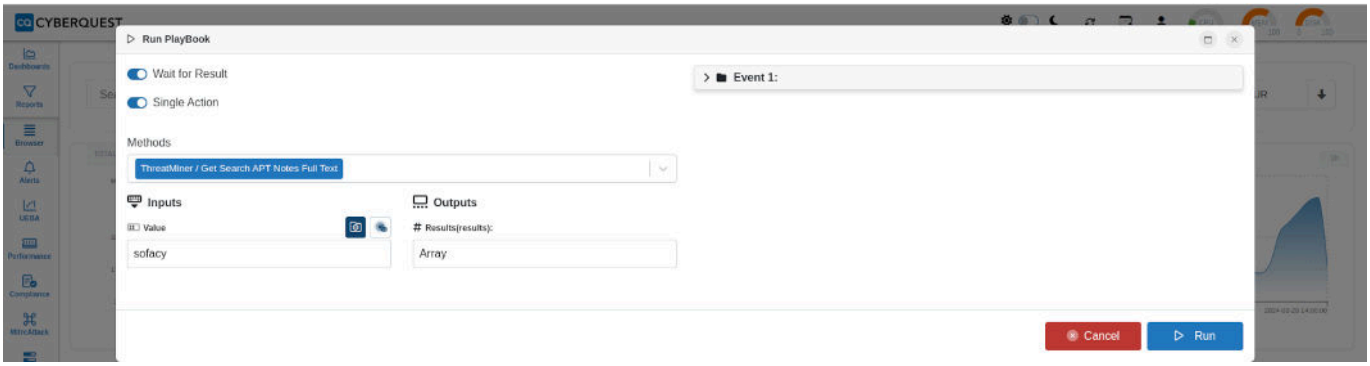


Inputs	Description
Value (is required)	The value which is used for this call

Outputs	Description
Results (results)	The results of the API call

ThreatMiner/Get Search APT Notes Full Text method

Based on query, receive different reports.



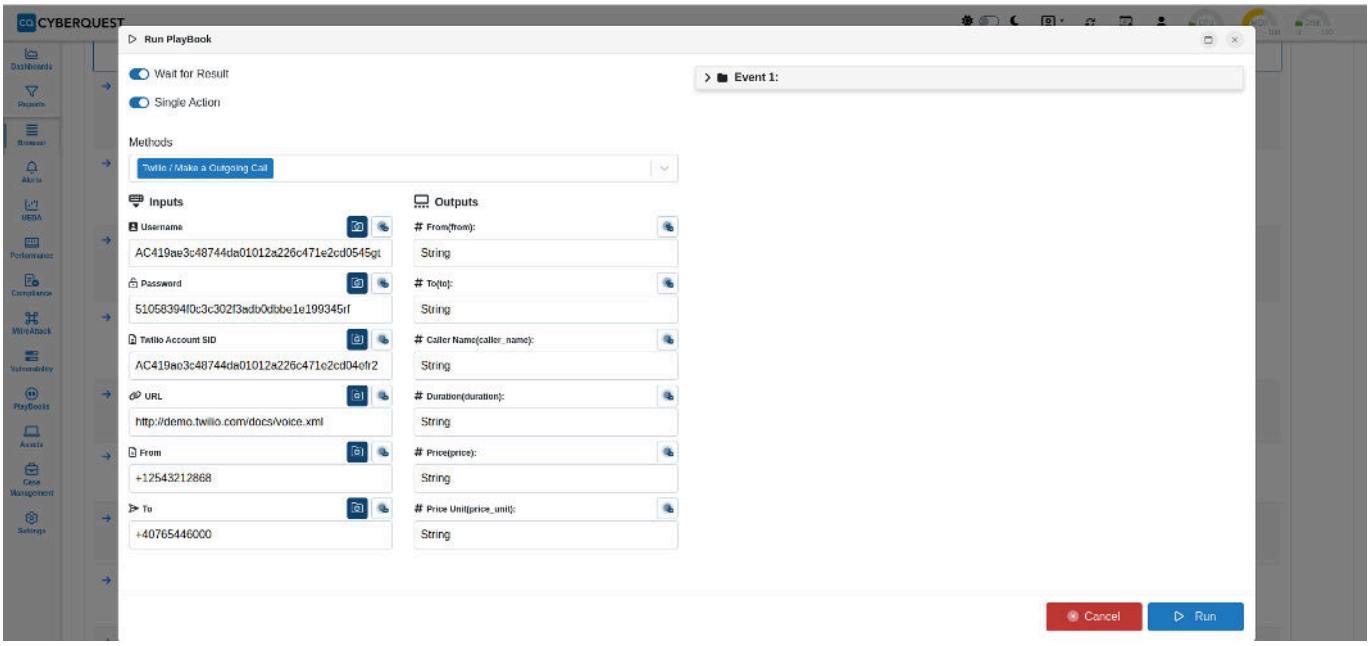
Inputs	Description
Value (is required)	The value which is used for this call

Outputs	Description
Results (results)	The results of the API call

Twilio

Twilio/Make a Outgoing Call method

Twilio is used to make an outgoing call from one phone to another.

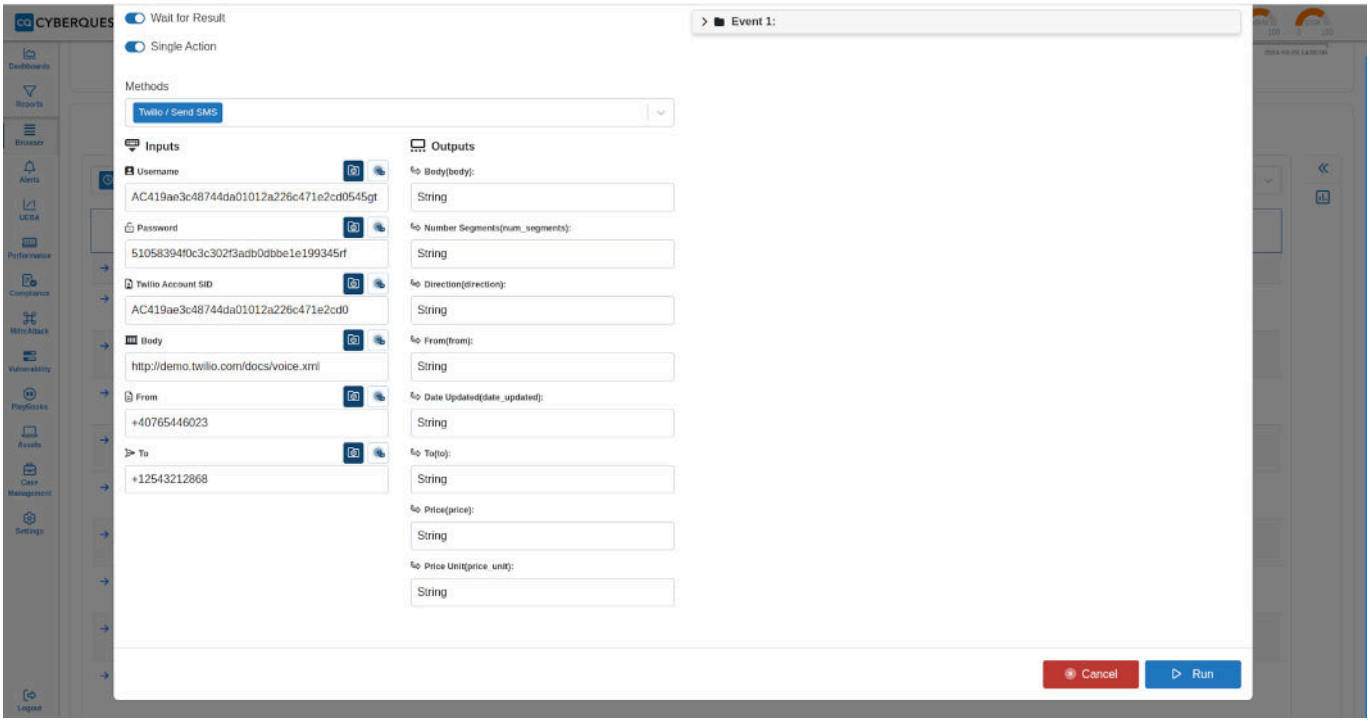


Inputs	Description
Username (is required)	Account SID
Password (is required)	Auth Token
Twilio Account SID (is required)	Account SID
URL (is required)	If you specify a URL parameter in your request, Twilio will make its HTTP request to this URL to retrieve TwiML to handle the call.
From (is required)	Twilio uses the From parameter (required) to set a phone number or client identifier as the caller ID for your outbound call.
To (is required)	The To parameter (required) is the phone number, SIP address, or client identifier you're calling.

Outputs	Description
From (from)	The Twilio phone number who calls
To (to)	The phone number who receives the call
Caller Name (caller_name)	Details about the caller name
Duration (duration)	The duration of the call
Price (price)	The call cost after executing the API
Price Unit (price_unit)	The currency

Twilio/Send SMS method

Twilio is used to send an SMS message from one phone to another.



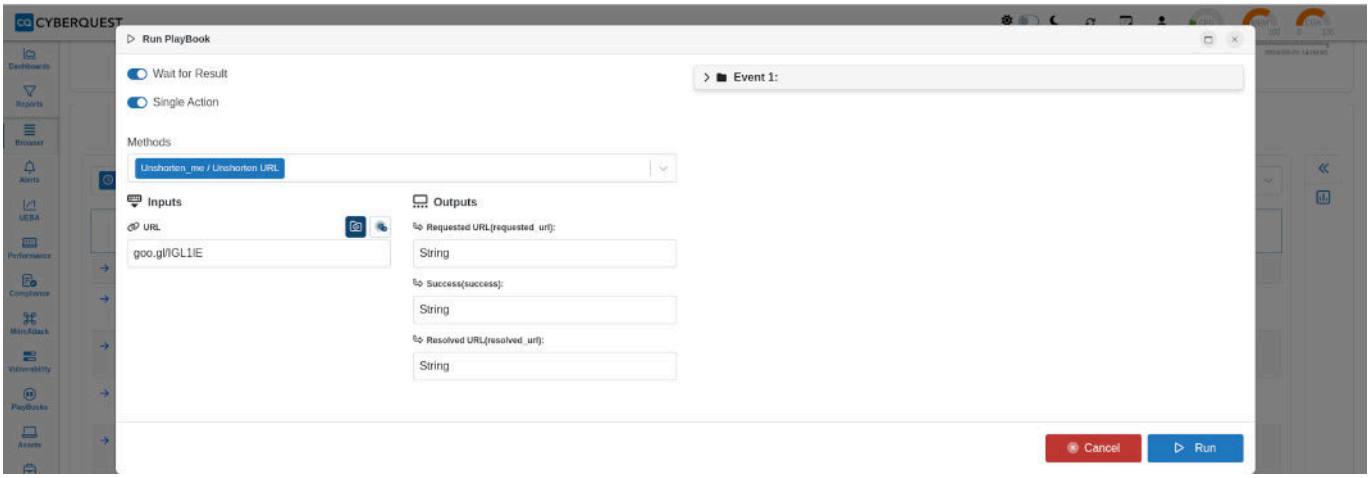
Inputs	Description
Username (is required)	Account SID
Password (is required)	Auth Token
Twilio Account SID (is required)	Account SID
Body (is required)	The body of this POST
From (is required)	From specifies the Twilio phone number, short code, or Messaging Service that sends this message. This must be a Twilio phone number that you own
To (is required)	This parameter determines the destination phone number for your SMS message.

Outputs	Description
Body (body)	The message send
Number Segments (num_segments)	The number of segments
Direction (direction)	The method used to call the API
From (from)	The Twilio phone number that sent the message
Date Updated (date_updated)	The timestamp when the API was last time updated
To (to)	The phone number that received the message
Price (price)	The cost of sending a message using the API
Price Unit (price_unit)	The currency

Unshorten.me

Unshorten_me/Unshorten URL method

Un-shorten URLs created by different services.



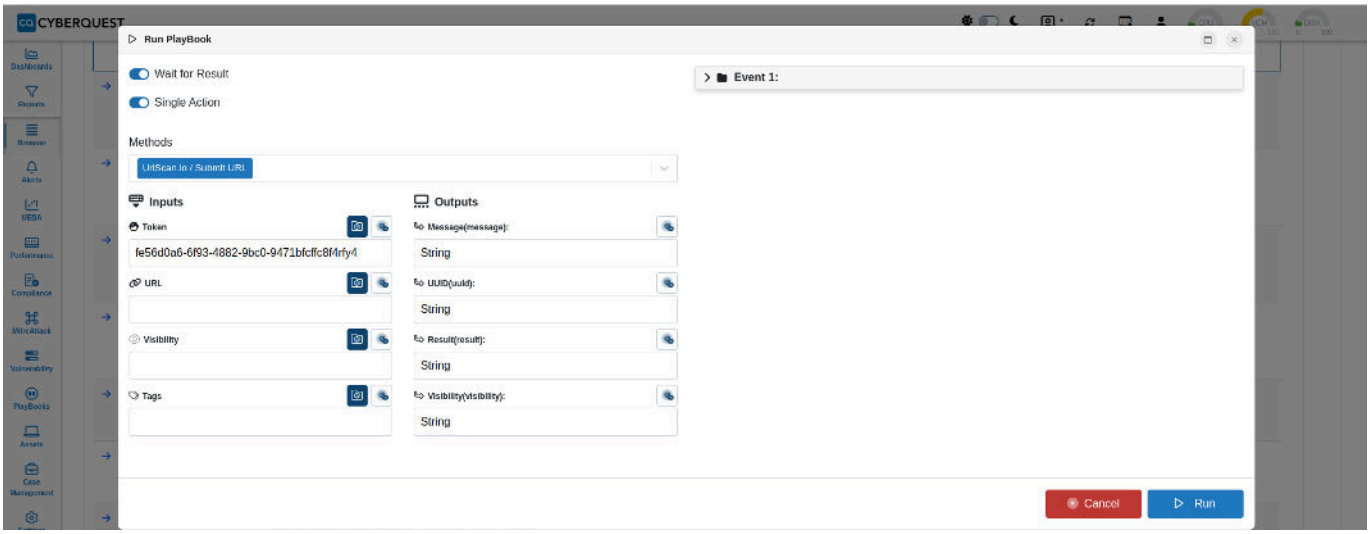
Inputs	Description
URL (is required)	The URL for which the execution takes place

Outputs	Description
Requested URL (requested_url)	The URL that is shortened
Success (success)	The status of the API call
Resolved URL (resolved_url)	The URL that is unshortened

UrlScan.io

UrlScan.io/Submit URL method

The submission API allows you to submit a URL to be scanned and set some options for the scan.

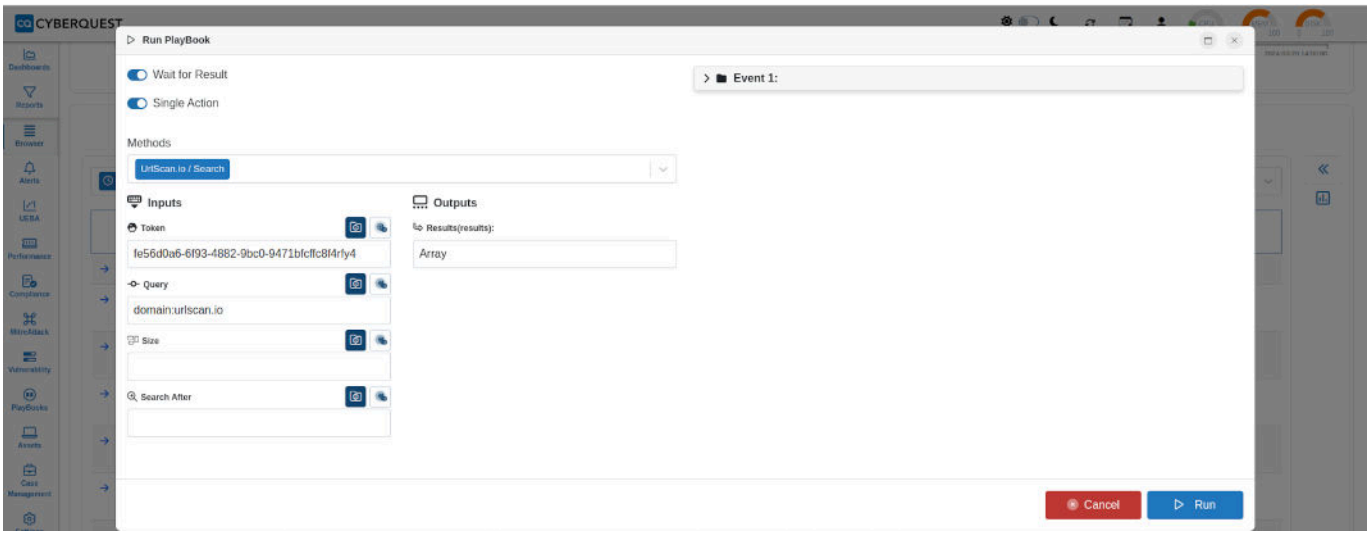


Inputs	Description
Token (is required)	To use the UrlScan.io API, you must have an API key.
URL	The URL which will be submitted
Visibility	The visibility of submission
Tags	User-defined tags to annotate this scan, e.g.: phishing or malicious. Limited to 10 tags.

Outputs	Description
Message (message)	The status of the API call
UUID (uuid)	The uuid generated generated after calling the APi
Result (result)	The link to the submission
Visibility (visibility)	The visibility of raport

UrlScan.io/Search method

The result has high-level metadata about the scan result and a link to the API for the full scan result.

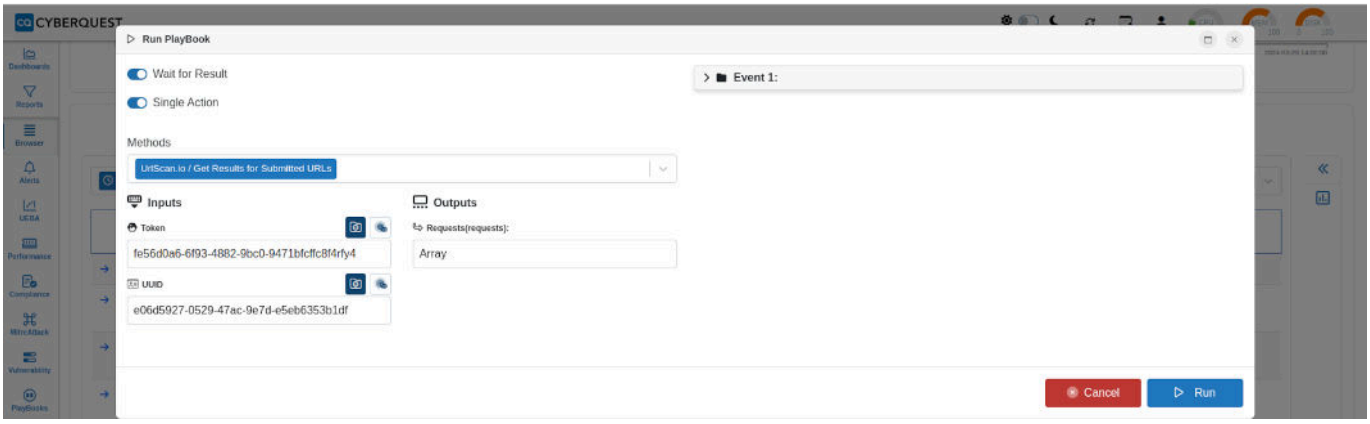


Inputs	Description
Token (is required)	To use the UrlScan.io API, you must have an API key.
Query (is required)	The query term (ElasticSearch Query String Query).
Size	Number of results returned. Default: 100, Max: 10000 (depending on your subscription)
Search After	For retrieving the next batch of results, value of the sort attribute of the last (oldest) result you received (comma-separated)

Outputs	Description
Results (results)	The results of the investigation

UrlScan.io/Get Results for Submitted URLs method

Receive results from url submitted.



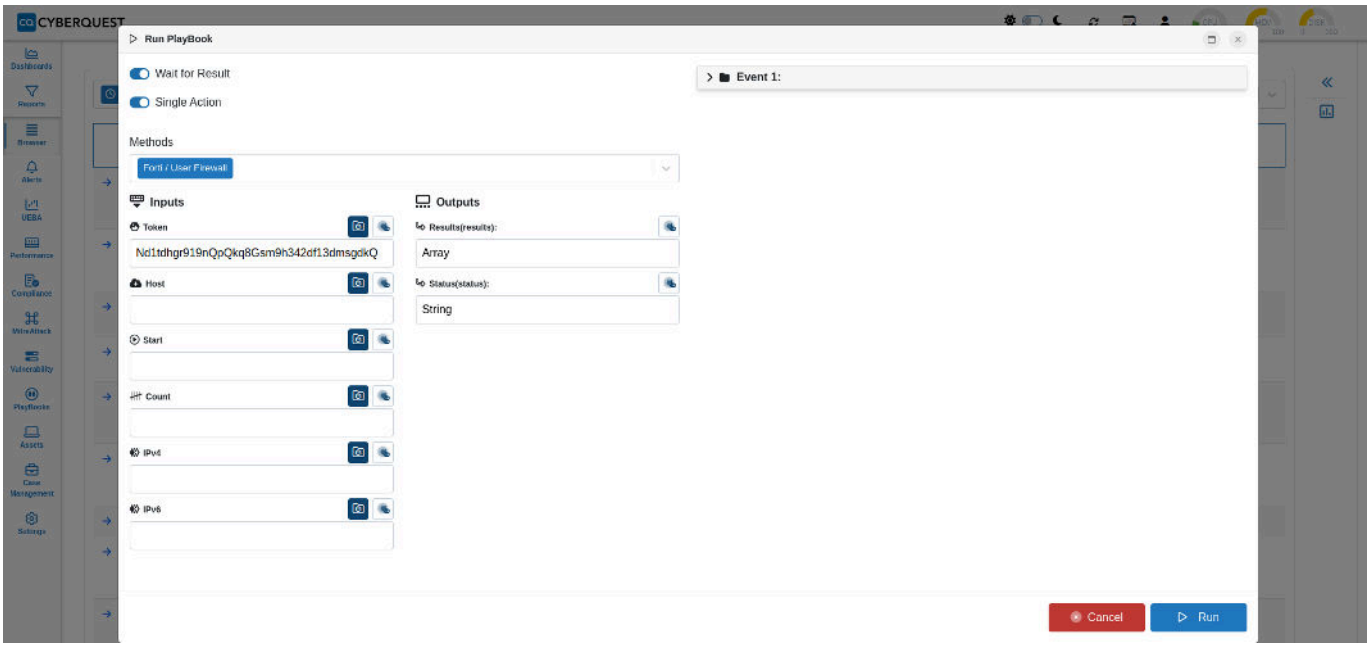
Inputs	Description
Token (is required)	To use the UrlScan.io API, you must have an API key.
UUID (is required)	Identify URL based on UUID

Outputs	Description
Requests (requests)	The list of requests to the investigated URL

Forti

Forti/User Firewall method

List authenticated firewall users.

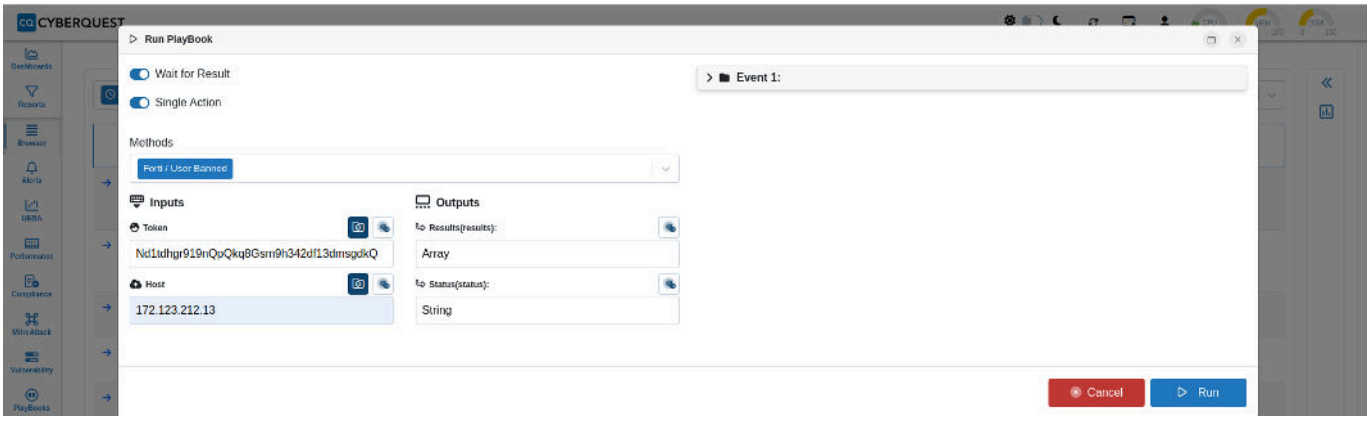


Inputs	Description
Token (is required)	To use the FortiOS API, you must have an API key
Host	Your FortiGate hostname
Start	Starting entry index
count	Maximum number of entries to return
IPv4	Include IPv4 user (default=true)
IPv6	Include IPv6 users

Outputs	Description
Results(results)	The results of the API call
Status(status)	Success if the API call was executed correctly

Forti/User Banned method

Return a list of all banned users by IP.

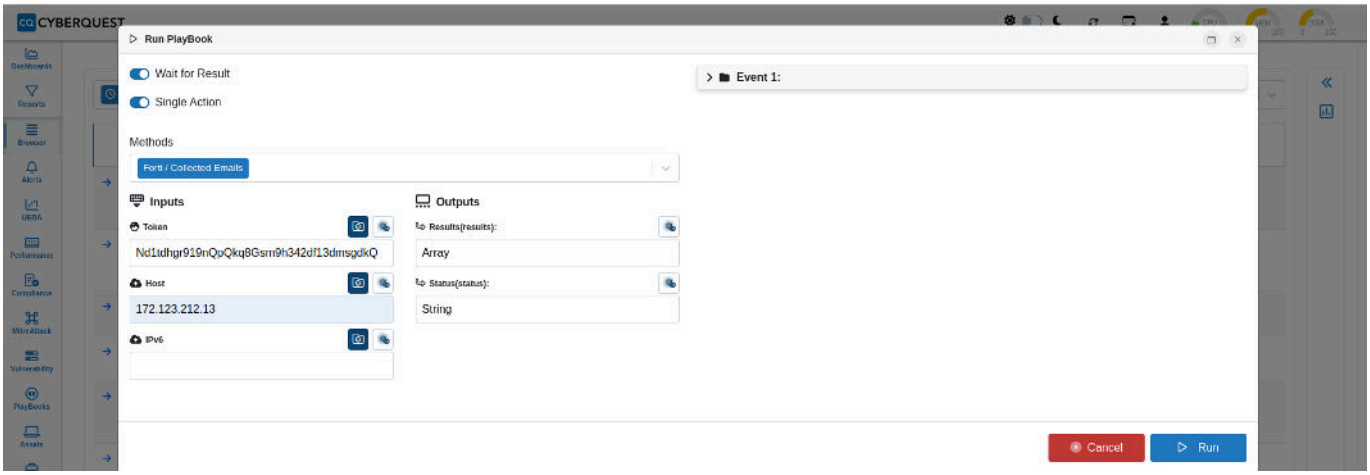


Inputs	Description
Token (is required)	To use the FortiOS API, you must have an API key
Host (is required)	Your FortiGate hostname

Outputs	Description
Results(results)	The results of the API call
Status(status)	Success if the API call was executed correctly

Forti/Collected Emails method

List email addresses collected from captive portal.

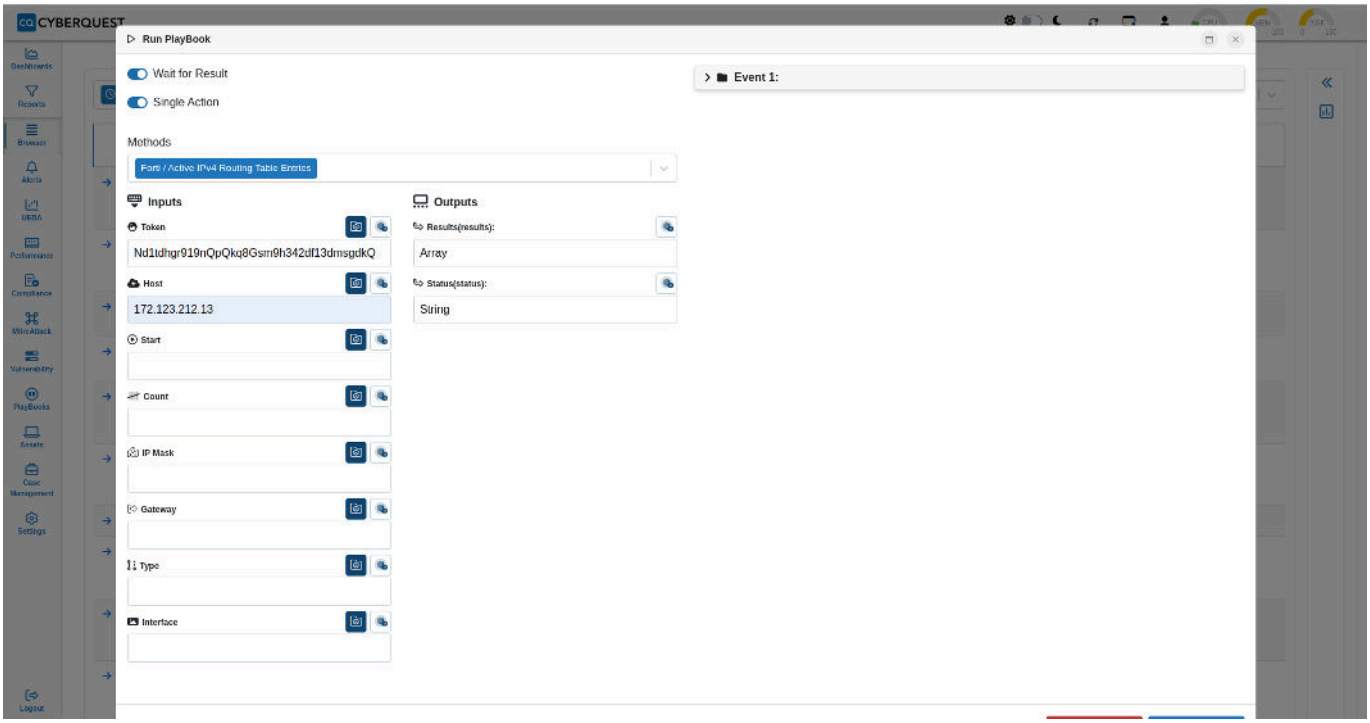


Inputs	Description
Token (is required)	To use the FortiOS API, you must have an API key
Host (is required)	Your FortiGate hostname

Outputs	Description
Results(results)	The results of the API call
Status(status)	Success if the API call was executed correctly

Forti/Active IPv4 Routing Table Entries method

List all active IPv4 routing table entries.

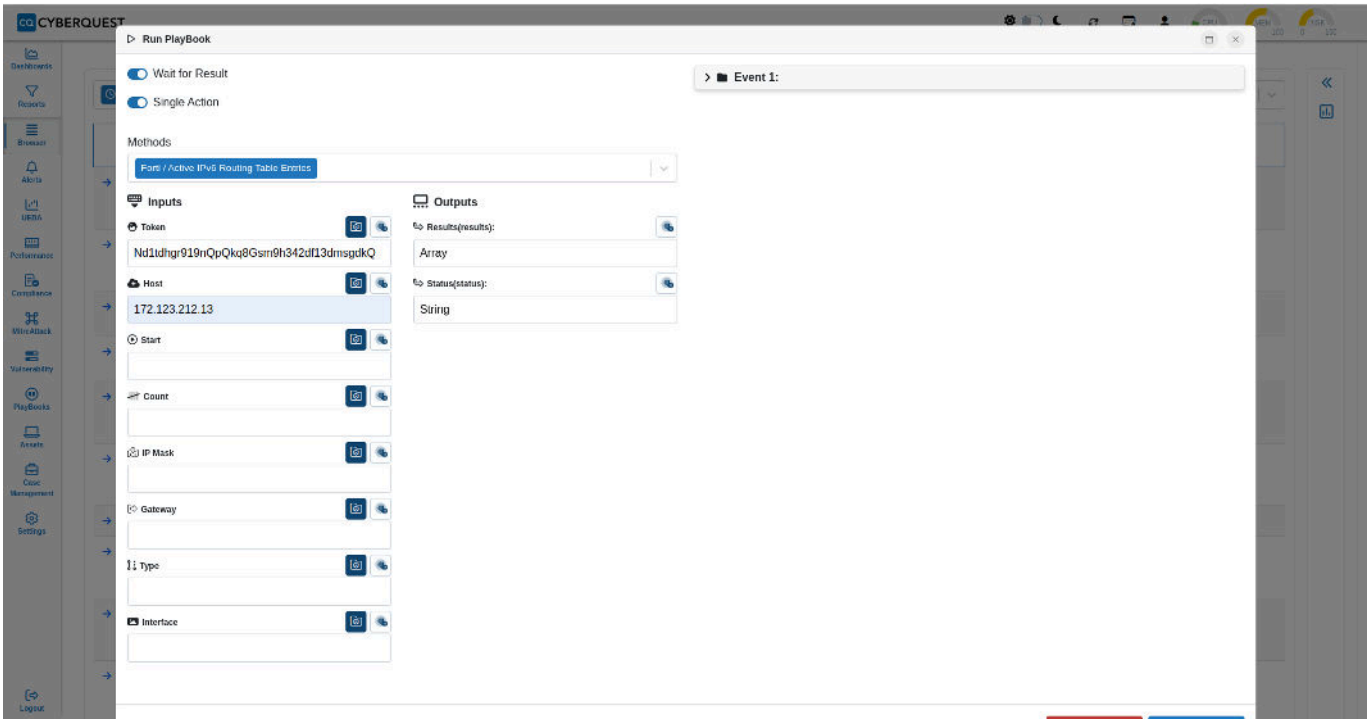


Inputs	Description
Token (is required)	To use the FortiOS API, you must have an API key
Host (is required)	Your FortiGate hostname
Start	Starting entry index
Count	Maximum number of entries to return (Default for all routes)
IP Mask	Filter: IP/netmask
Gateway	Filter: gateway
Type	Filter: route type
Interface	Filter: interface name

Outputs	Description
Results(results)	The results of the API call
Status(status)	Success if the API call was executed correctly

Forti/Active IPv6 Routing Table Entries method

List all active IPv6 routing table entries.

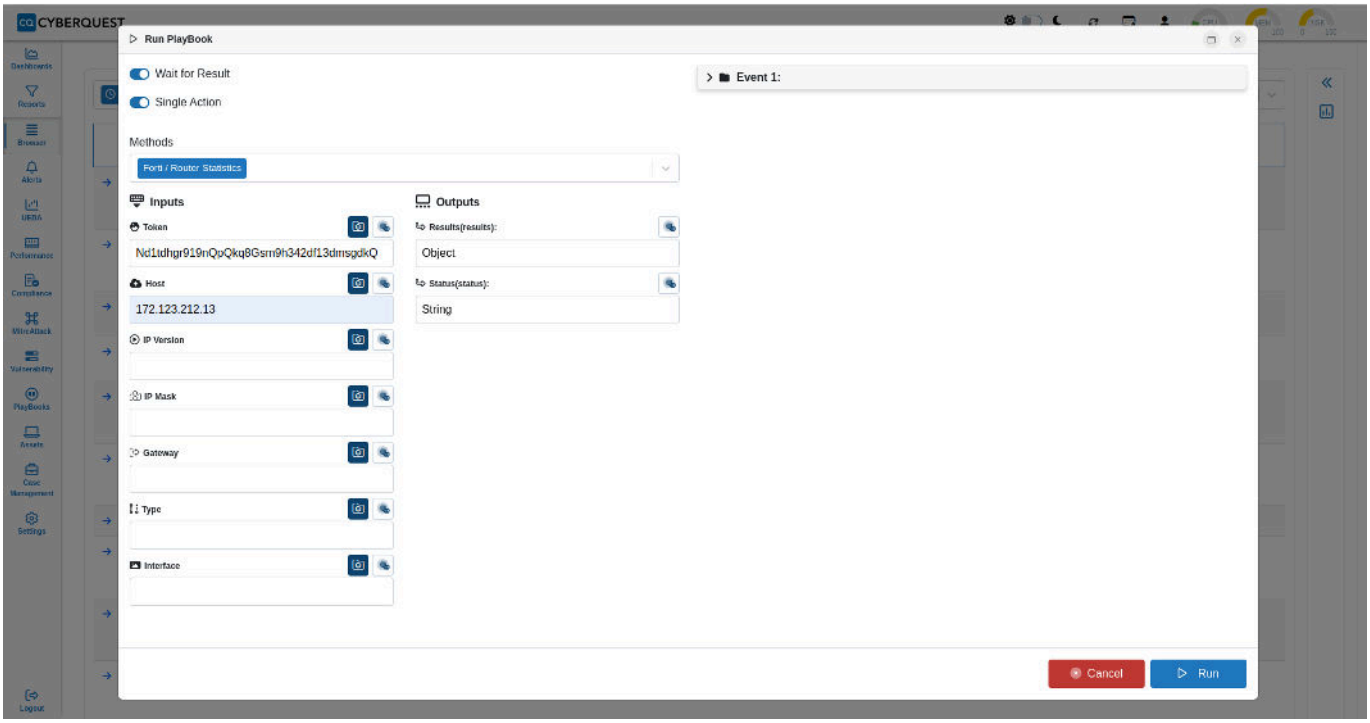


Inputs	Description
Token (is required)	To use the FortiOS API, you must have an API key
Host (is required)	Your FortiGate hostname
Start	Starting entry index
Count	Maximum number of entries to return (Default for all routes)
IP Mask	Filter: IP/netmask
Gateway	Filter: gateway
Type	Filter: route type
Interface	Filter: interface name

Outputs	Description
Results(results)	The results of the API call
Status(status)	Success if the API call was executed correctly

Forti/Router Statistics method

Retrieve routing table statistics, including number of matched routes.

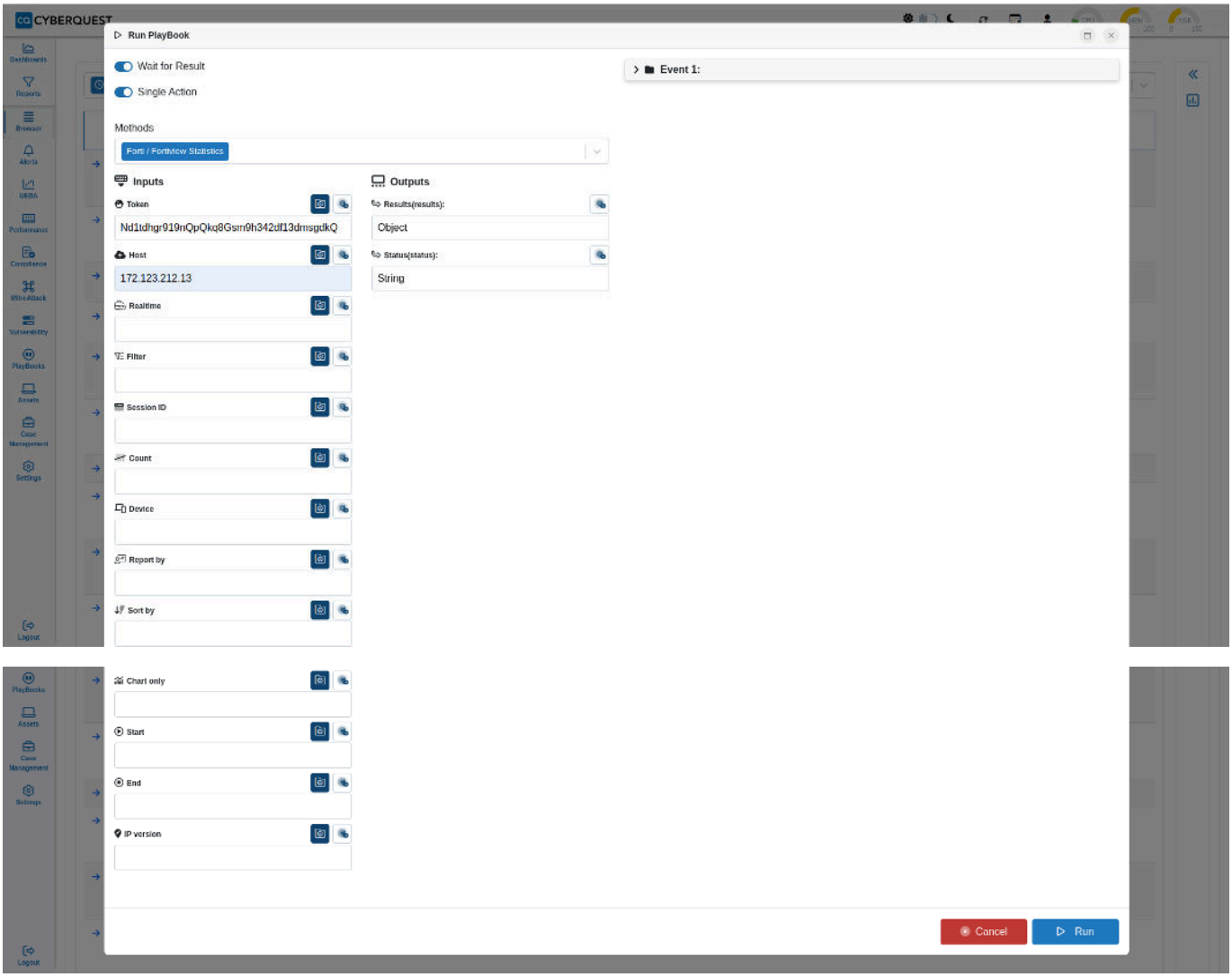


Inputs	Description
Token (is required)	To use the FortiOS API, you must have an API key
Host (is required)	Your FortiGate hostname
Start	IP version (4/6). If not present, IPv4 and IPv6 will be returned
Count	Filter: IP/netmask
IP Mask	Filter: gateway
Gateway	Filter: route type
Type	Filter: interface name
Interface	

Outputs	Description
Results(results)	The results of the API call
Status(status)	Success if the API call was executed correctly

Forti/Fortiview Statistics method

Retrieve drill-down and summary data for FortiView (both realtime and historical).

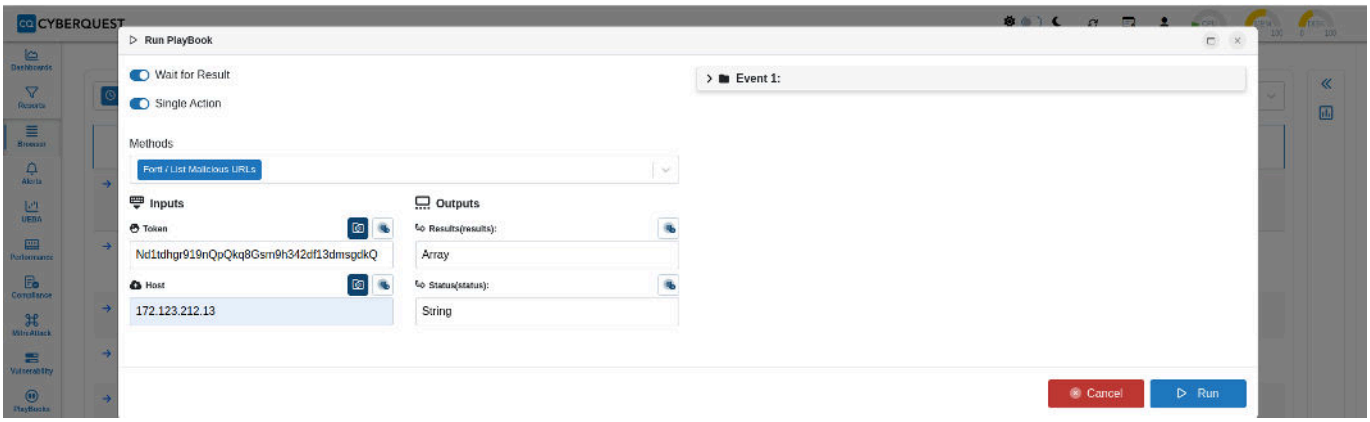


Inputs	Description
Token (is required)	To use the FortiOS API, you must have an API key
Host (is required)	Your FortiGate hostname
Realtime	Set to true to retrieve realtime results (from kernel)
Filter	A map of filter keys to arrays of values
Session ID	FortiView request Session ID
Count	Maximum number of entries to return
Device	FortiView source device [disk/fortianalyzer/forticloud]
Report by	Report by field
Sort by	Sort by field
Chart only	Only return graph values in results
Start	Start timestamp
End	End timestamp
IP version	IP version [*ipv4 / ipv6 / ipboth]

Outputs	Description
Results(results)	The results of the API call
Status(status)	Success if the API call was executed correctly

Forti/List Malicious URLs method

List all URLs in FortiSandbox malicious URL database.

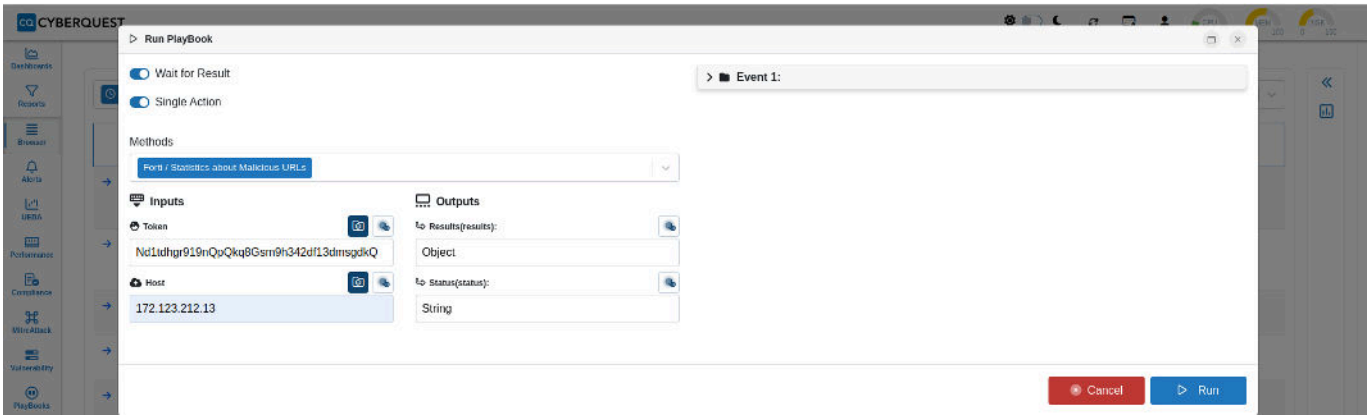


Inputs	Description
Token (is required)	To use the FortiOS API, you must have an API key
Host (is required)	Your FortiGate hostname

Outputs	Description
Results(results)	The results of the API call
Status(status)	Success if the API call was executed correctly

Forti/Statistics about Malicious URLs method

Retrieve statistics for the FortiSandbox malicious URL database.

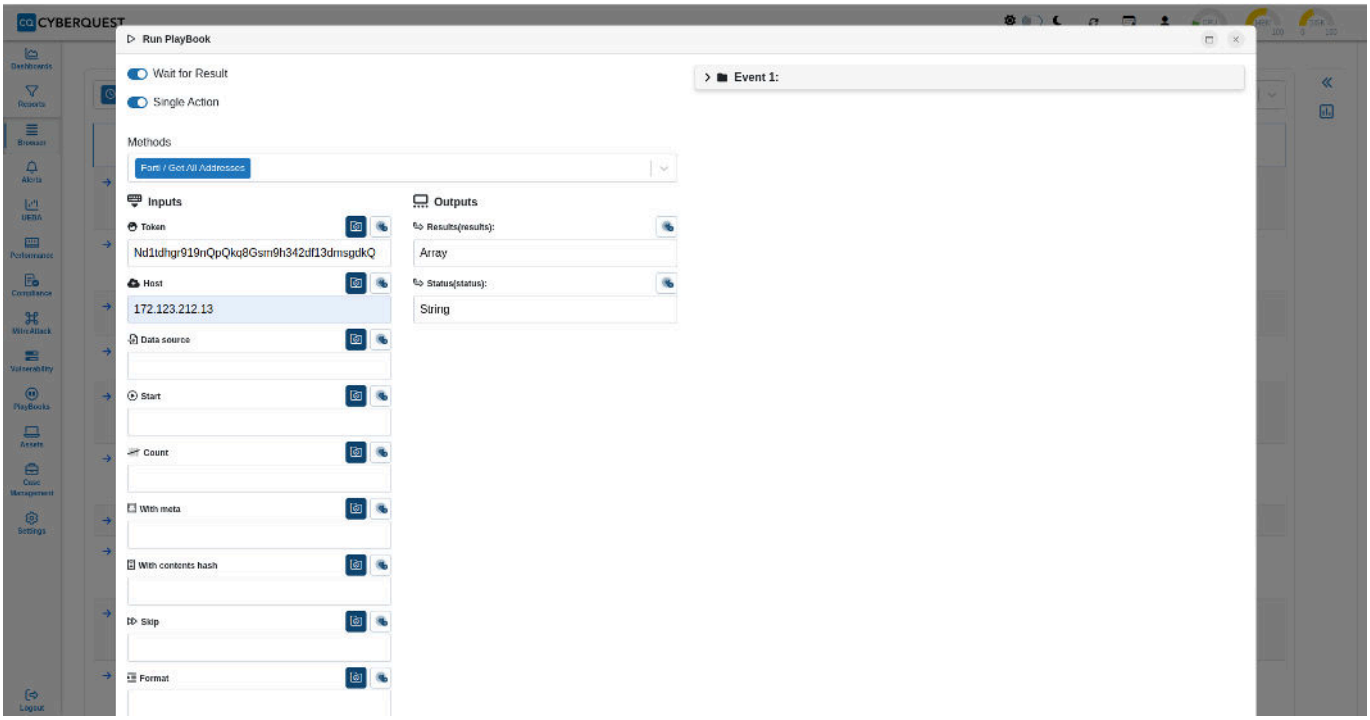


Inputs	Description
Token (is required)	To use the FortiOS API, you must have an API key
Host (is required)	Your FortiGate hostname

Outputs	Description
Results(results)	The results of the API call
Status(status)	Success if the API call was executed correctly

Forti/Get All Addresses method

Return all Addresses created.

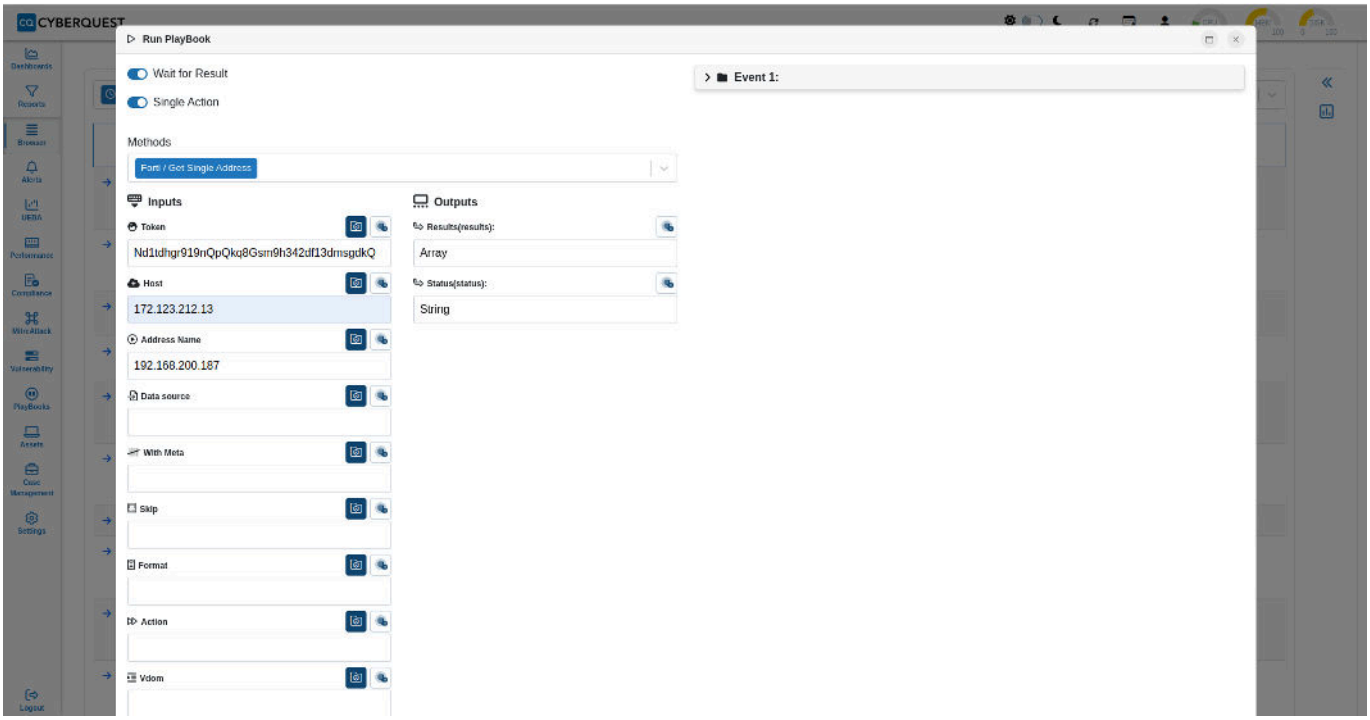


Inputs	Description
Token (is required)	To use the FortiOS API, you must have an API key.
Host (is required)	Your FortiGate hostname
Data source	Enable to include datasource information for each linked object.
Start	Starting entry index.
Count	Maximum number of entries to return.
With meta	Enable to include meta information about each object (type id, references, etc).
With contents hash	Enable to include a checksum of each objects contents.
Skip	Enable to call CLI skip operator to hide skipped properties.
Format	List of property names to include in results, separated by
Filter	Filtering multiple key/value pairsOperator
Key	If present, objects will be filtered on property with this name.
Pattern	If present, objects will be filtered on property with this value.
Scope	Scope [global
Exclude default values	Exclude properties/objects with default value
Action	default: Return the CLI default values for entire CLI tree.meta: Return meta data for a specific object, table, or the entire CLI tree.schema: Return schema for entire CLI tree.
VDOM	Specify the Virtual Domain(s) from which results are returned or changes are applied to. If this parameter is not provided, the management VDOM will be used. If the admin does not have access to the VDOM, a permission error will be returned.The URL parameter is one of:vdom=root (Single VDOM)vdom=vdom1,vdom2 (Multiple VDOMs)vdom=* (All VDOMs)

Outputs	Description
Results(results)	The results of the API call
Status(status)	Success if the API call was executed correctly

Forti/Get Single Address method

Select a single address by name.

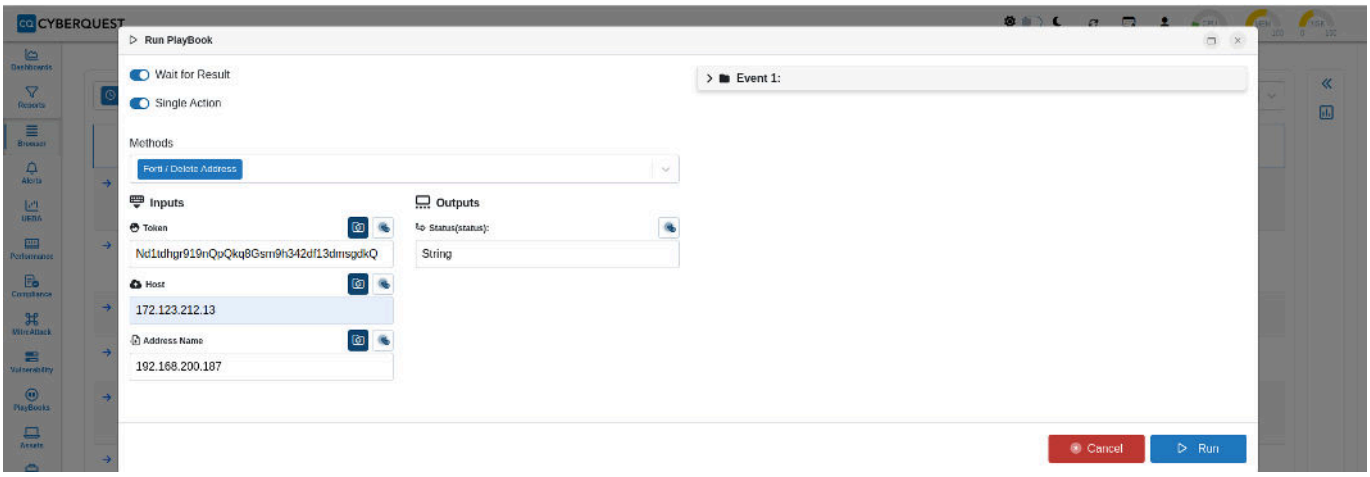


Inputs	Description
Token (is required)	To use the FortiOS API, you must have an API key.
Host (is required)	Your FortiGate hostname
Address Name (is required)	The address name which will be searched
Data source	Enable to include datasource information for each linked object.
With Meta	Enable to include meta information about each object (type id, references, etc).
Skip	Enable to call CLI skip operator to hide skipped properties.
Format	List of property names to include in results, separated by
Action	default: Return the CLI default values for this object type.schema: Return the CLI schema for this object type.revision: Return the CMDB revision for this object type.transaction-list: List all configuration transaction(s).
Vdom	Specify the Virtual Domain(s) from which results are returned or changes are applied to. If this parameter is not provided, the management VDOM will be used. If the admin does not have access to the VDOM, a permission error will be returned.The URL parameter is one of:vdom=root (Single VDOM)vdom=vdom1,vdom2 (Multiple VDOMs)vdom=* (All VDOMs)

Outputs	Description
Results (results)	The results of the API call
Status(status)	Success if the API call was executed correctly

Forti/Delete Address method

Delete an Address.

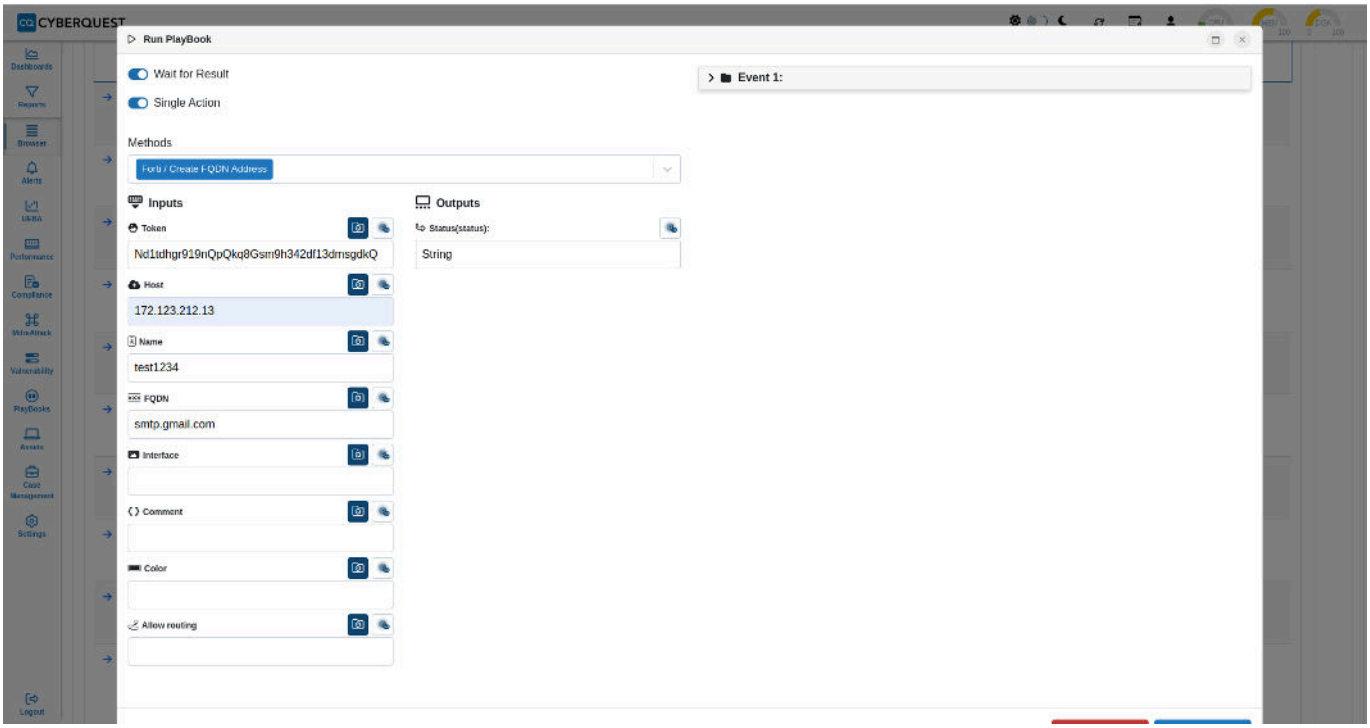


Inputs	Description
Token (is required)	To use the FortiOS API, you must have an API key.
Host (is required)	Your FortiGate hostname
Address Name (is required)	The name of the address

Outputs	Description
Status (status)	Success if the API call was executed correctly

Forti/Create FQDN Address method

Create a FQDN Address.

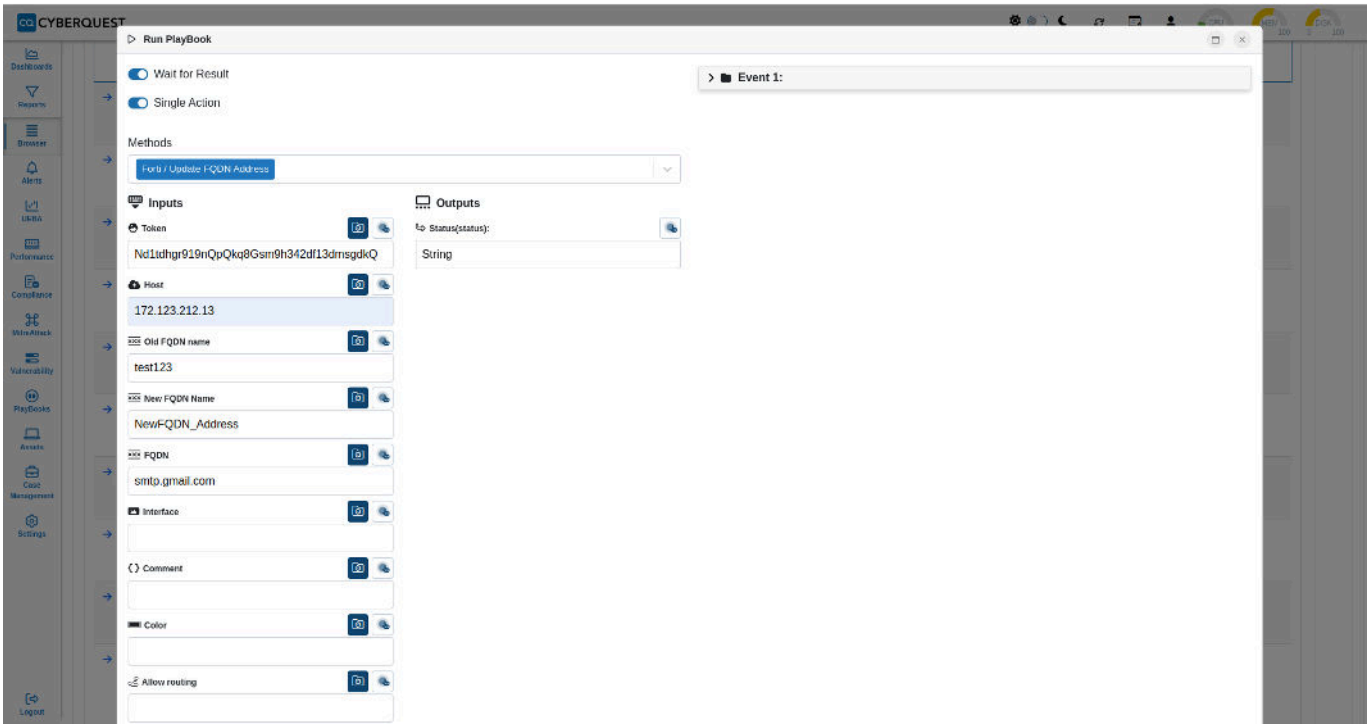


Inputs	Description
Token (is required)	To use the FortiOS API, you must have an API key.
Host (is required)	Your FortiGate hostname
Name (is required)	Address name. To execute with success this API call you need to provide a unique name (which is not already existing in your FortiGate)
FQDN (is required)	Fully Qualified Domain Name address
Interface	Name of interface whose IP address is to be used.
Comment	Write a short description about this Address
Color	Color of icon on the GUI.
Allow routing	Enable/disable use of this address in the static route configuration.enable:Enable use of this address in the static route configuration.disable:Disable use of this address in the static route configuration.

Outputs	Description
Status (status)	Success if the API call was executed correctly

Forti/Update FQDN Address method

Update a FQDN Address.

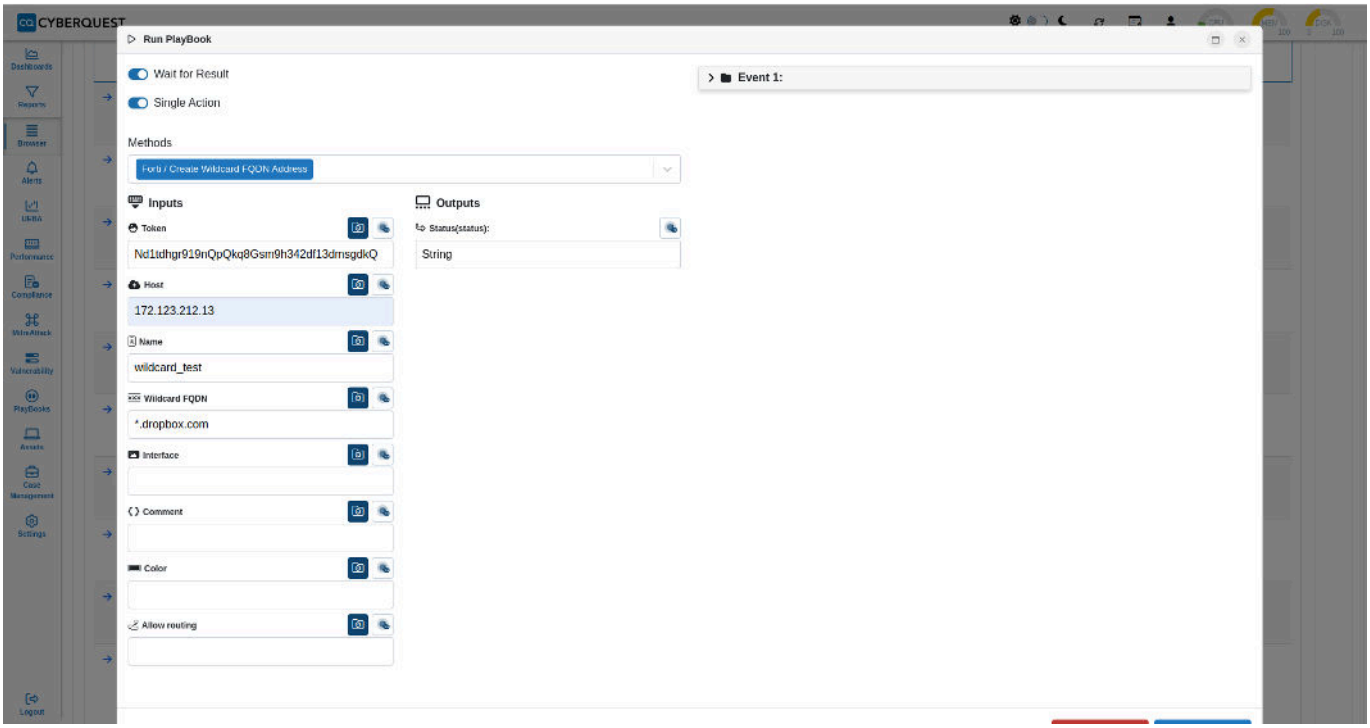


Inputs	Description
Token (is required)	To use the FortiOS API, you must have an API key.
Host (is required)	Your FortiGate hostname
Old FQDN name (is required)	The FQDN name which will be changed
New FQDN Name (is required)	Address name
FQDN	Fully Qualified Domain Name address
Interface	Name of interface whose IP address is to be used.
Comment	Write a short description about this Address
Color	Color of icon on the GUI.
Allow routing	Enable/disable use of this address in the static route configuration.enable:Enable use of this address in the static route configuration.disable:Disable use of this address in the static route configuration.

Outputs	Description
Status (status)	Success if the API call was executed correctly

Forti/Create Wildcard FQDN Address method

Create a Wildcard FQDN Address.

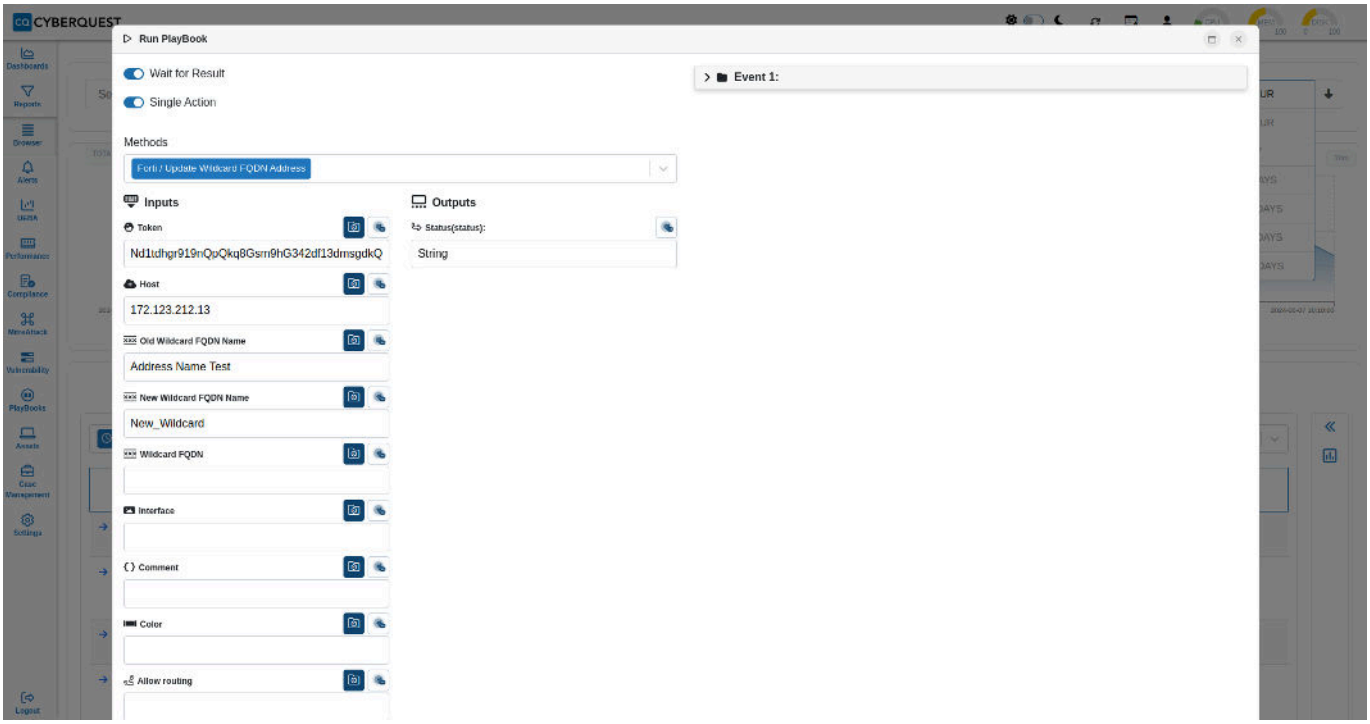


Inputs	Description
Token (is required)	To use the FortiOS API, you must have an API key.
Host (is required)	Your FortiGate hostname
Name (is required)	Address name.To execute with success this API call you need to provide a unique name (which is not already existing in your FortiGate)
Wildcard FQDN (is required)	Fully Qualified Domain Name address
Interface	Name of interface whose IP address is to be used.
Comment	Write a short description about this Address
Color	Color of icon on the GUI.
Allow routing	Enable/disable use of this address in the static route configuration.enable:Enable use of this address in the static route configuration.disable:Disable use of this address in the static route configuration.

Outputs	Description
Status (status)	Success if the API call was executed correctly

Forti/Update Wildcard FQDN Address method

Update a Wildcard FQDN Address.

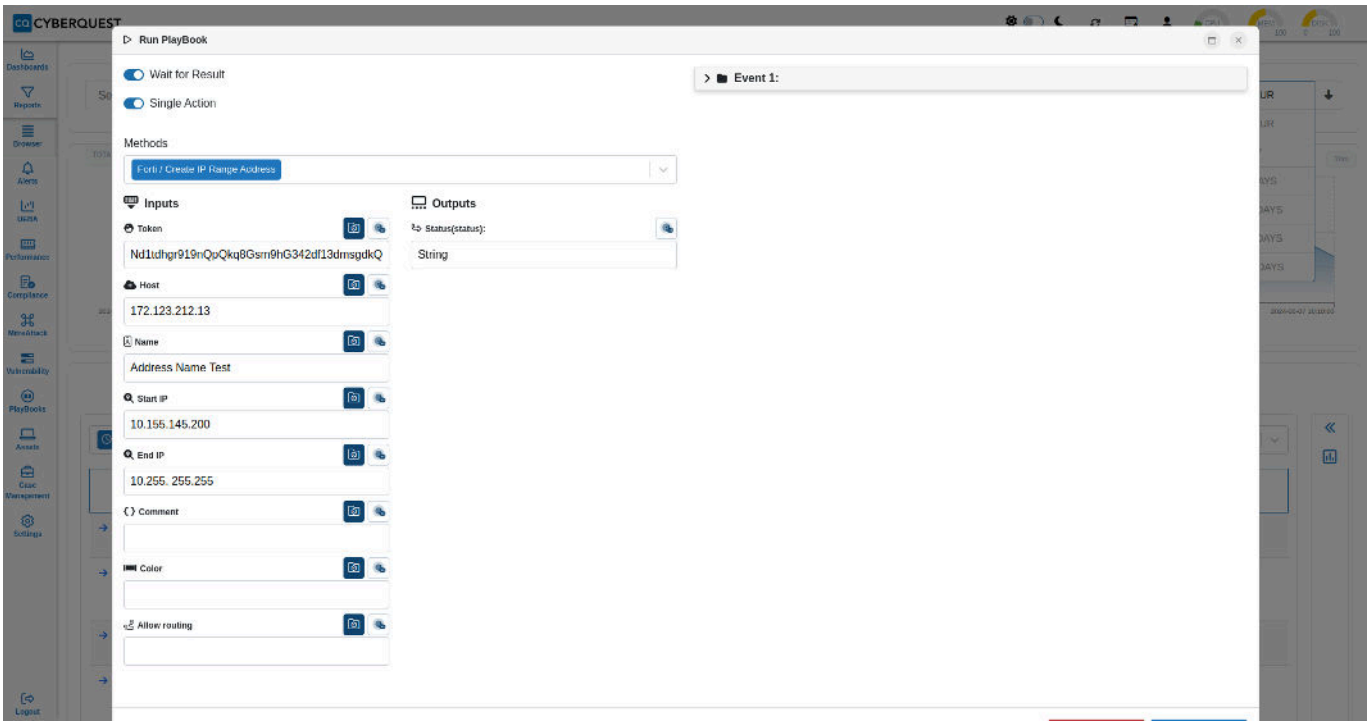


Inputs	Description
Token (is required)	To use the FortiOS API, you must have an API key.
Host (is required)	Your FortiGate hostname
Old Wildcard FQDN Name (is required)	The Wildcard FQDN Address name which will be changed
New Wildcard FQDN Name (is required)	Address name
Wildcard FQDN	Fully Qualified Domain Name address
Interface	Name of interface whose IP address is to be used.
Comment	Write a short description about this Address
Color	Color of icon on the GUI.
Allow routing	Enable/disable use of this address in the static route configuration.enable:Enable use of this address in the static route configuration.disable:Disable use of this address in the static route configuration.

Outputs	Description
Status (status)	Success if the API call was executed correctly

Forti/Create IP Range Address method

Create IP Range Address.

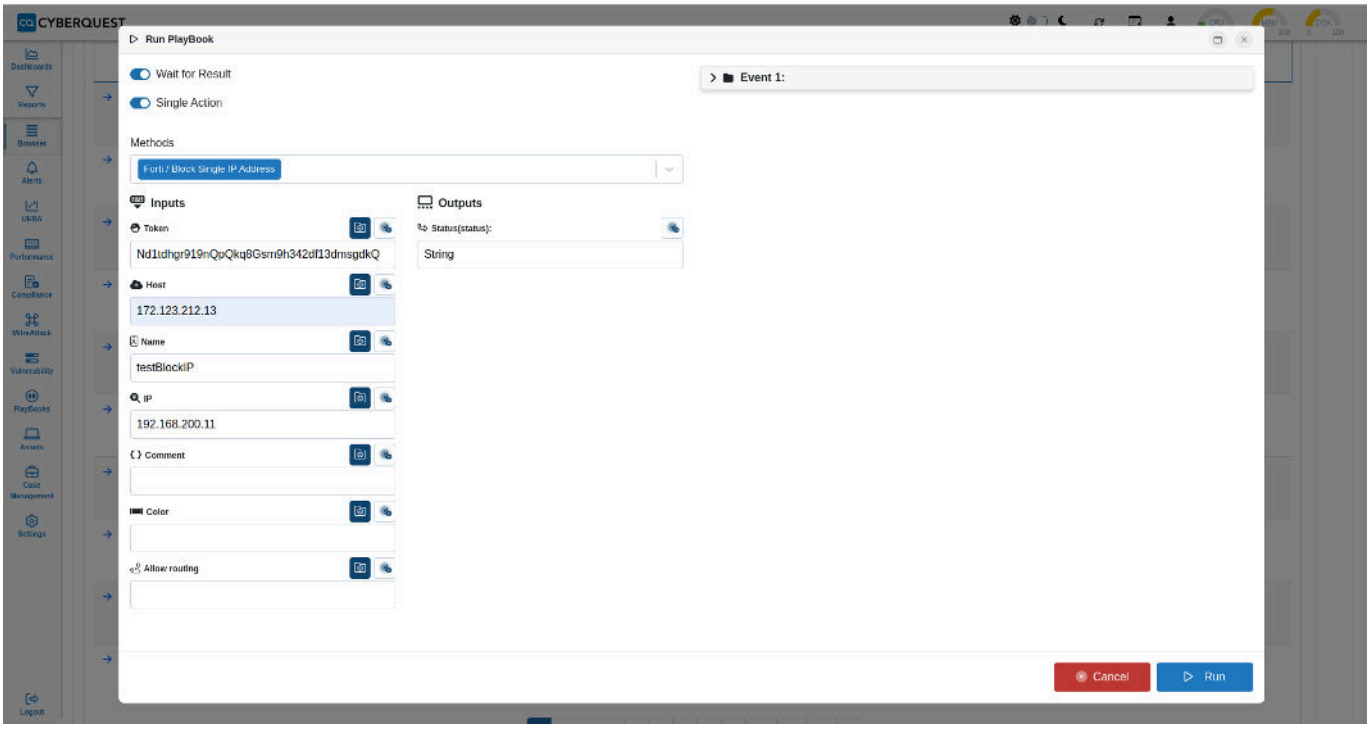


Inputs	Description
Token (is required)	To use the FortiOS API, you must have an API key.
Host (is required)	Your FortiGate hostname
Name (is required)	Address name. To execute with success this API call you need to provide a unique name (which is not already existing in your FortiGate)
Start IP (is required)	First IP address (inclusive) in the range for the address.
End IP (is required)	Final IP address (inclusive) in the range for the address.
Comment	Write a short description about this Address
Color	Color of icon on the GUI.
Allow routing	Enable/disable use of this address in the static route configuration.enable:Enable use of this address in the static route configuration.disable:Disable use of this address in the static route configuration.

Outputs	Description
Status (status)	Success if the API call was executed correctly

Forti/Block Single IP Address method

Block Single IP Address.

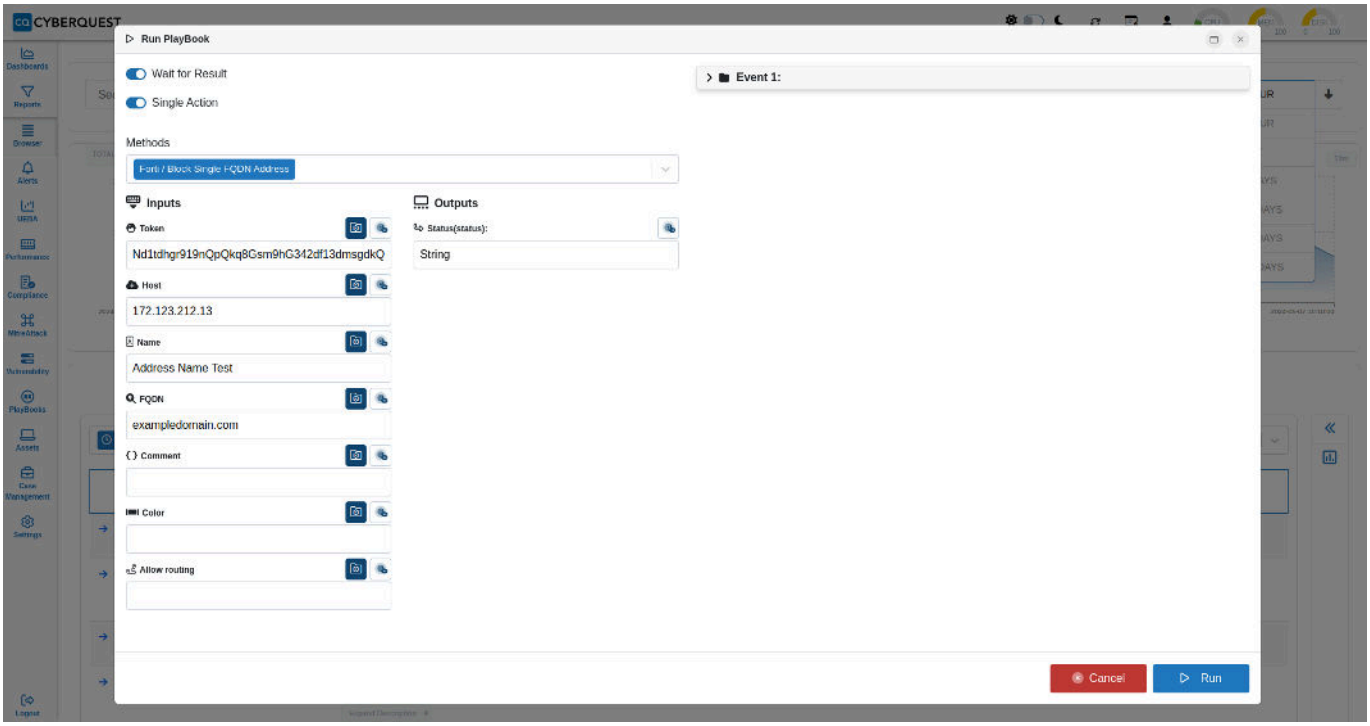


Inputs	Description
Token (is required)	To use the FortiOS API, you must have an API key.
Host (is required)	Your FortiGate hostname
Name (is required)	Address name
IP (is required)	The IP which will be used to create the address
Comment	Write a short description about this Address
Color	Color of icon on the GUI.
Allow routing	Enable/disable use of this address in the static route configuration.enable:Enable use of this address in the static route configuration.disable:Disable use of this address in the static route configuration.

Outputs	Description
Status (status)	Success if the API call was executed correctly

Forti/Block Single FQDN Address method

Create Single FQDN Address.

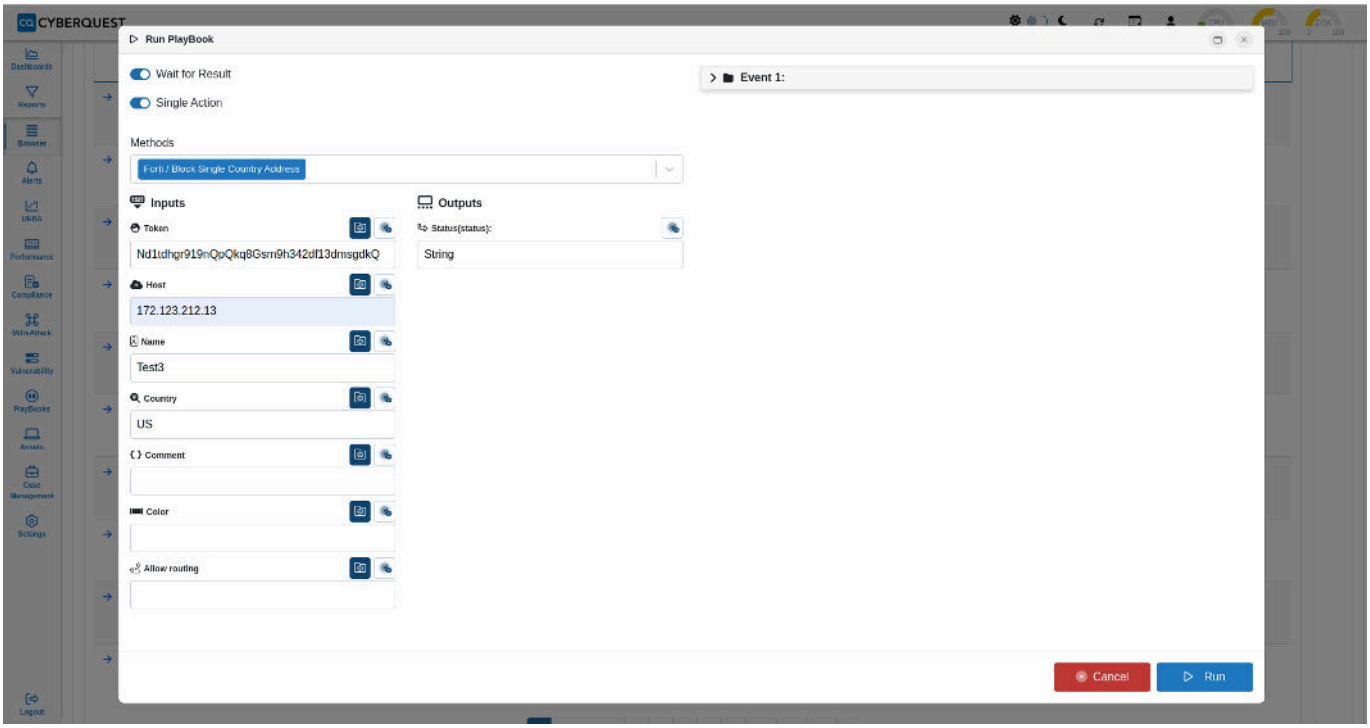


Inputs	Description
Token (is required)	To use the FortiOS API, you must have an API key.
Host (is required)	Your FortiGate hostname
Name (is required)	Address name
FQDN (is required)	The FQDN which will be used to create the address
Comment	Write a short description about this Address
Color	Color of icon on the GUI.
Allow routing	Enable/disable use of this address in the static route configuration.enable:Enable use of this address in the static route configuration.disable:Disable use of this address in the static route configuration.

Outputs	Description
Status (status)	Success if the API call was executed correctly

Forti/Block Single Country Address method

Create Single Country Address.

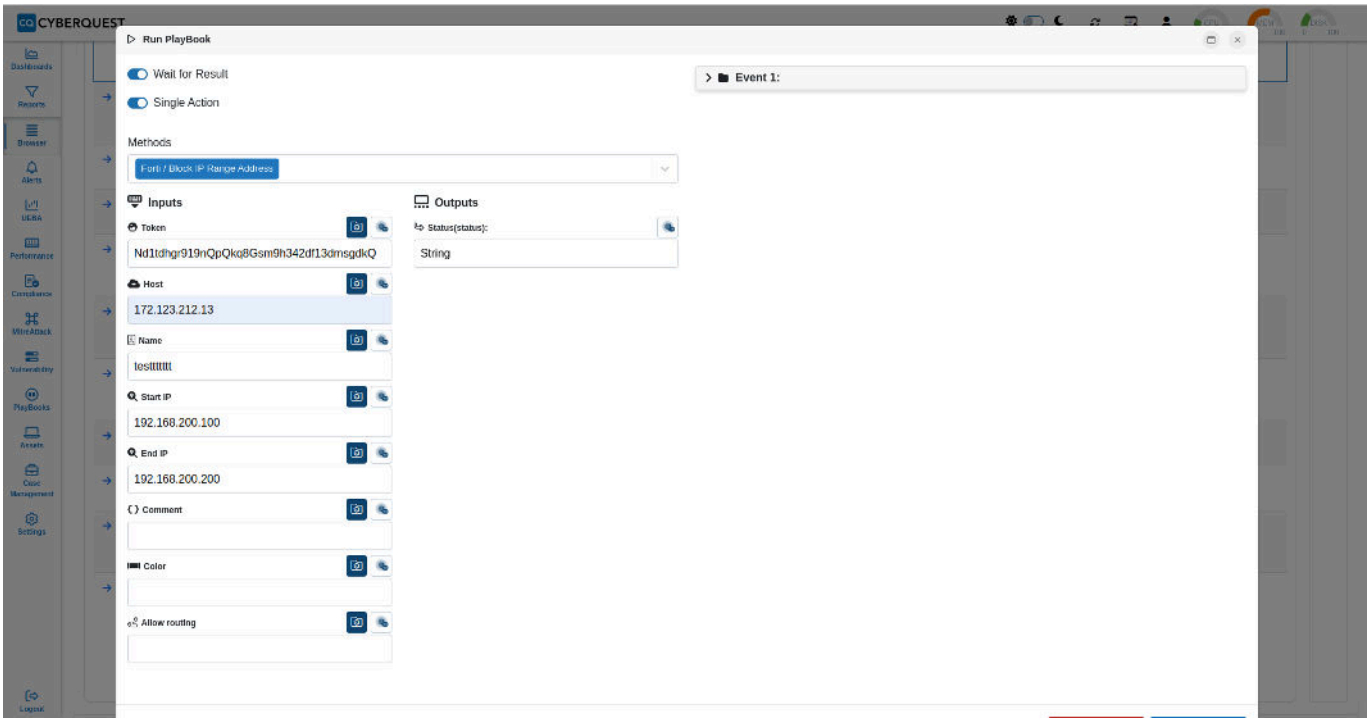


Inputs	Description
Token (is required)	To use the FortiOS API, you must have an API key.
Host (is required)	Your FortiGate hostname
Name (is required)	Address name
Country (is required)	The country which will be used to create the address. Use ISO 3166 notation for countries (ex: US)
Comment	Write a short description about this Address
Color	Color of icon on the GUI.
Allow routing	Enable/disable use of this address in the static route configuration.enable:Enable use of this address in the static route configuration.disable:Disable use of this address in the static route configuration.

Outputs	Description
Status (status)	Success if the API call was executed correctly

Forti/Block IP Range Address method

Block IP Range Address.

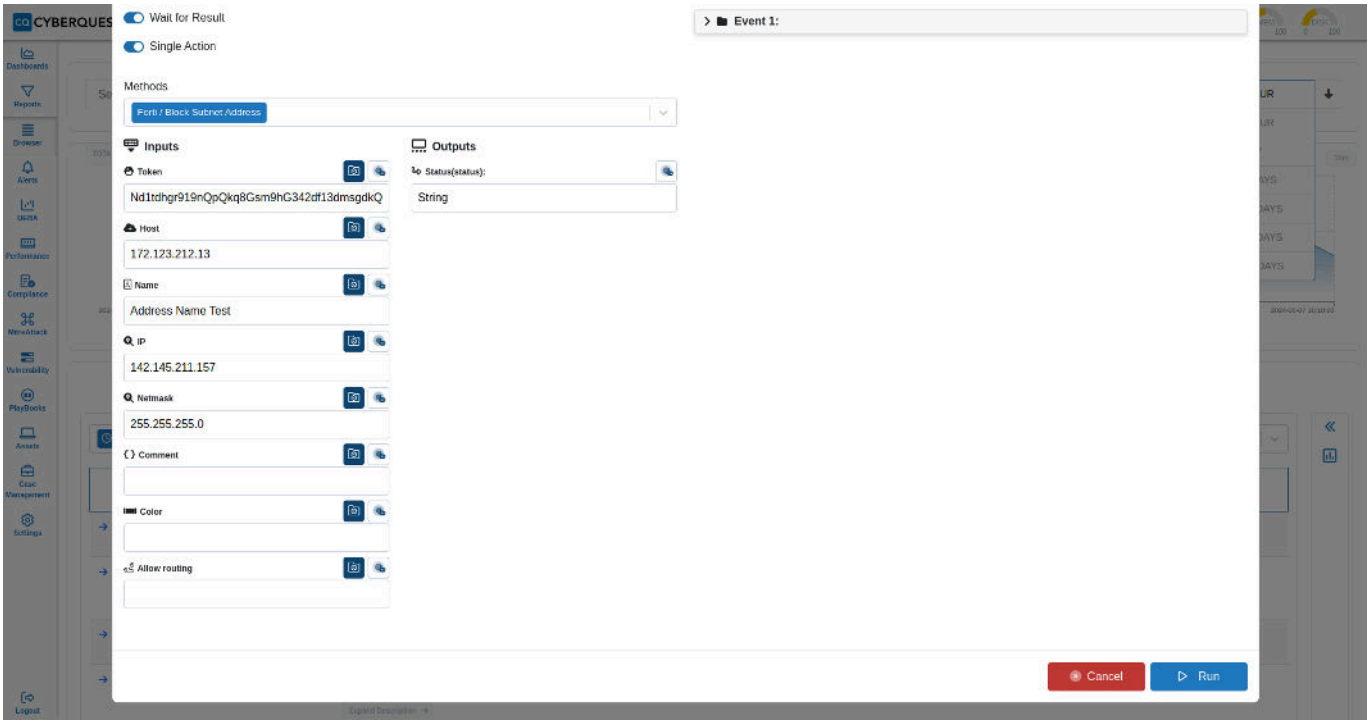


Inputs	Description
Token (is required)	To use the FortiOS API, you must have an API key.
Host (is required)	Your FortiGate hostname
Name (is required)	Address name
Start IP (is required)	The Start IP which will be used to create the address
End IP (is required)	The End IP which will be used to create the address
Comment	Write a short description about this Address
Color	Color of icon on the GUI.
Allow routing	Enable/disable use of this address in the static route configuration.enable:Enable use of this address in the static route configuration.disable:Disable use of this address in the static route configuration.

Outputs	Description
Status (status)	Success if the API call was executed correctly

Forti/Block Subnet Address method

Block Subnet Address.

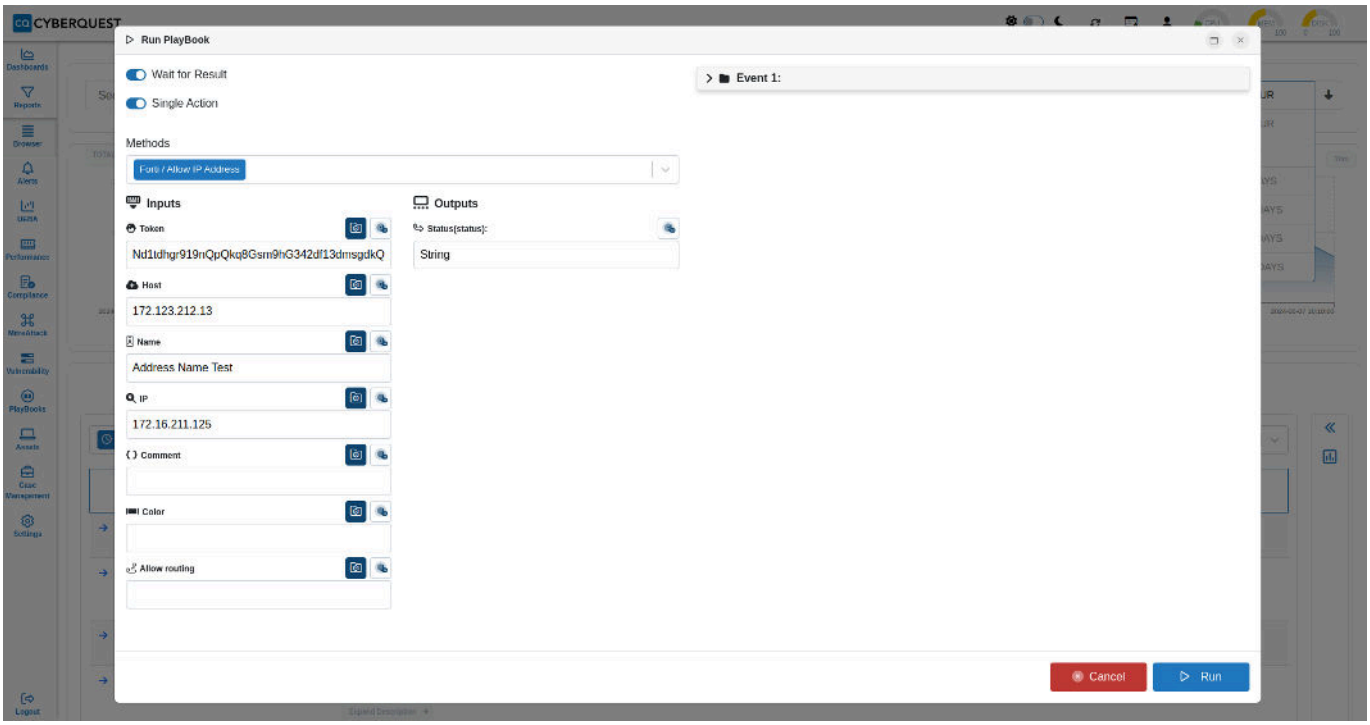


Inputs	Description
Token (is required)	To use the FortiOS API, you must have an API key.
Host (is required)	Your FortiGate hostname
Name (is required)	Address name
IP (is required)	The IP which will be used to create the address
Netmask (is required)	The Netmask which will be used to create the address
Comment	Write a short description about this Address
Color	Color of icon on the GUI.
Allow routing	Enable/disable use of this address in the static route configuration.enable:Enable use of this address in the static route configuration.disable:Disable use of this address in the static route configuration.

Outputs	Description
Status (status)	Success if the API call was executed correctly

Forti/Allow IP Address method

Allow Single IP Address.

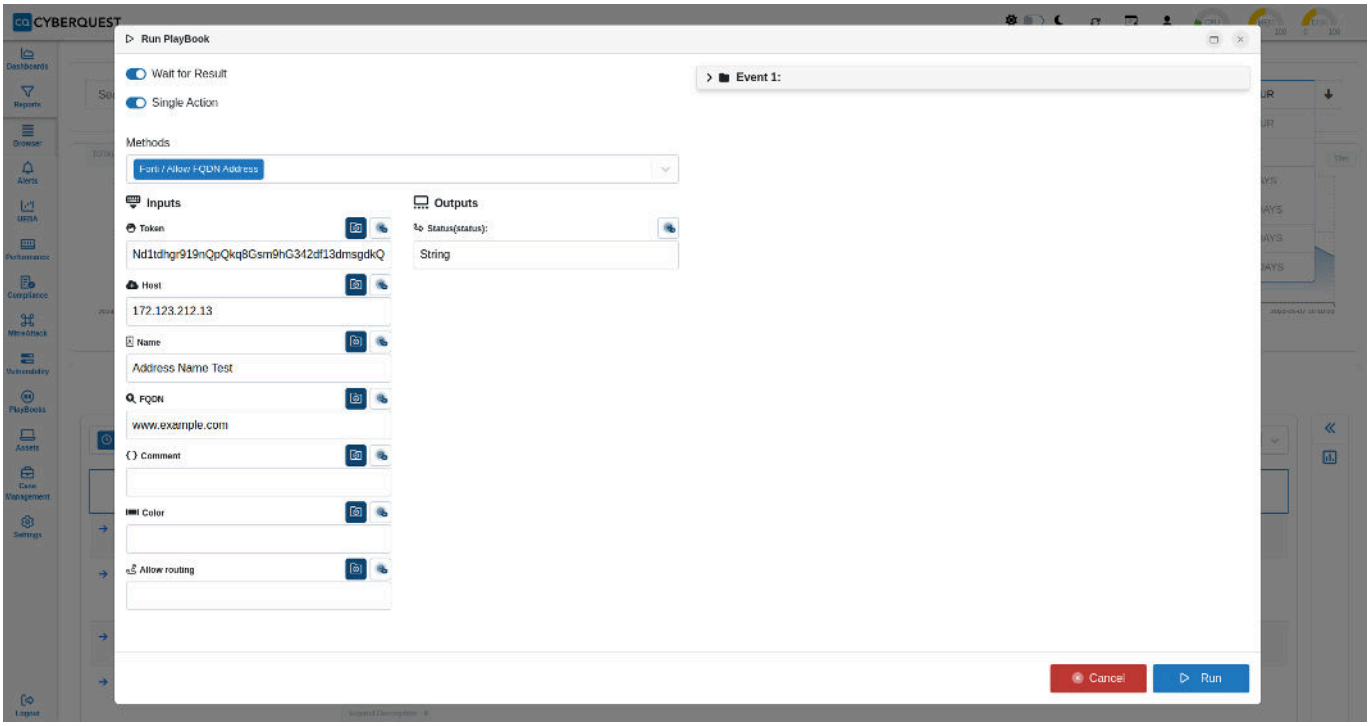


Inputs	Description
Token (is required)	To use the FortiOS API, you must have an API key.
Host (is required)	Your FortiGate hostname
Name (is required)	Address name
IP (is required)	The IP which will be used to create the address
Comment	Write a short description about this Address
Color	Color of icon on the GUI.
Allow routing	Enable/disable use of this address in the static route configuration.enable:Enable use of this address in the static route configuration.disable:Disable use of this address in the static route configuration.

Outputs	Description
Status (status)	Success if the API call was executed correctly

Forti/Allow FQDN Address method

Allow Single FQDN Address.

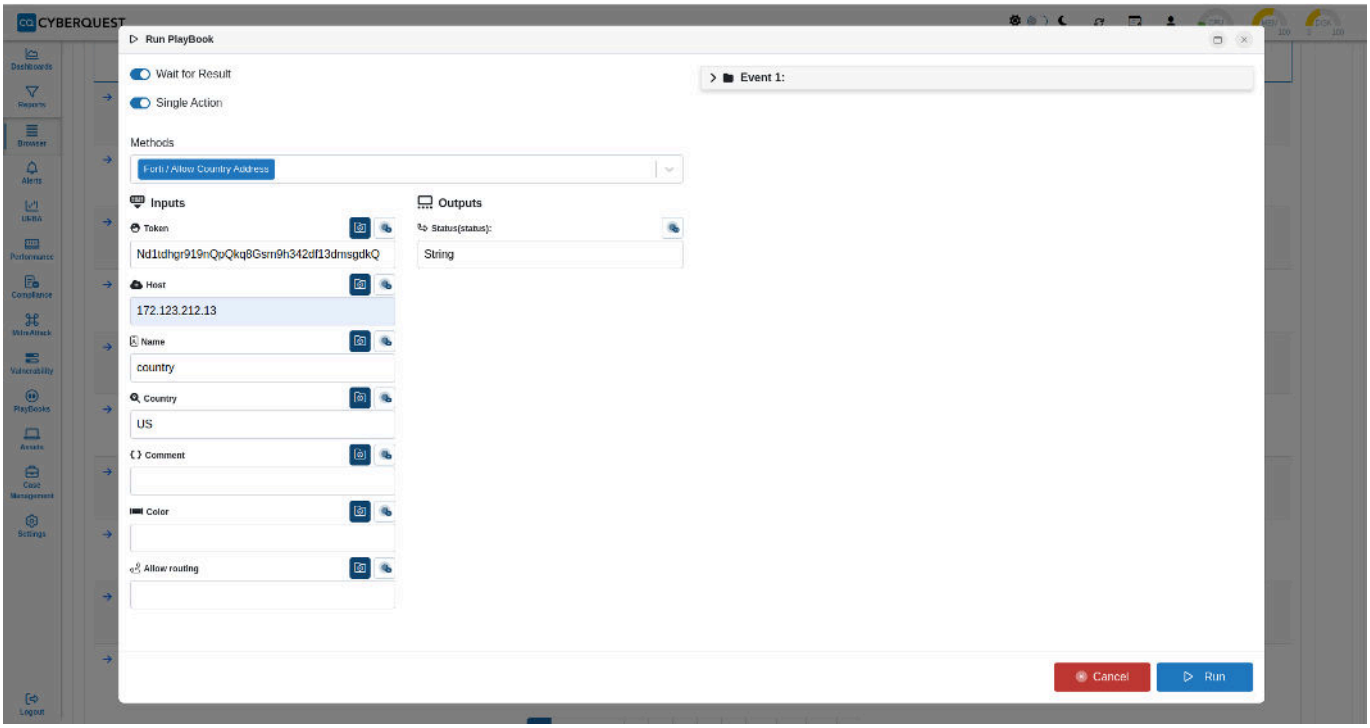


Inputs	Description
Token (is required)	To use the FortiOS API, you must have an API key.
Host (is required)	Your FortiGate hostname
Name (is required)	Address name
FQDN (is required)	The FQDN which will be used to create the address
Comment	Write a short description about this Address
Color	Color of icon on the GUI.
Allow routing	Enable/disable use of this address in the static route configuration.enable:Enable use of this address in the static route configuration.disable:Disable use of this address in the static route configuration.

Outputs	Description
Status (status)	Success if the API call was executed correctly

Forti/Allow Country Address method

Allow Single Country Address.

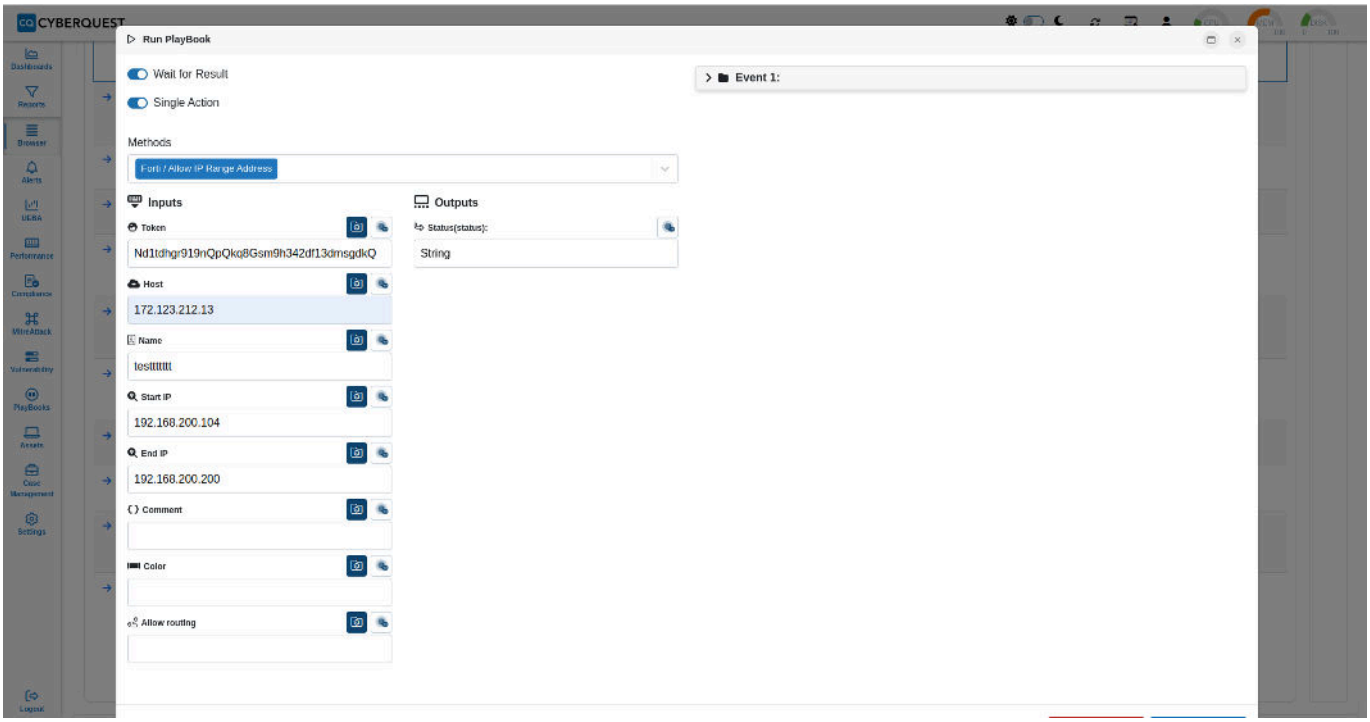


Inputs	Description
Token (is required)	To use the FortiOS API, you must have an API key.
Host (is required)	Your FortiGate hostname
Name (is required)	Address name
Country (is required)	The country which will be used to create the address. Use ISO 3166 notation for countries (ex: US)
Comment	Write a short description about this Address
Color	Color of icon on the GUI.
Allow routing	Enable/disable use of this address in the static route configuration.enable:Enable use of this address in the static route configuration.disable:Disable use of this address in the static route configuration.

Outputs	Description
Status (status)	Success if the API call was executed correctly

Forti/Allow IP Range Address method

Allow IP Range Address.

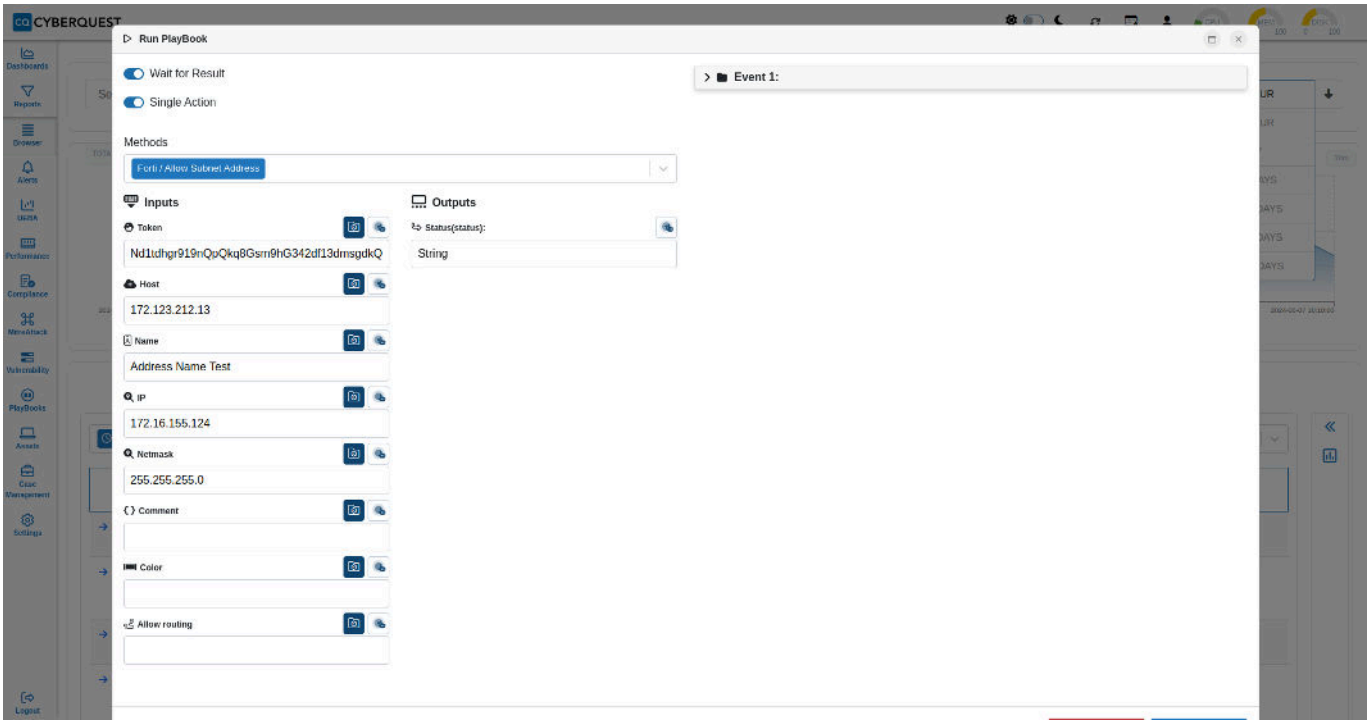


Inputs	Description
Token (is required)	To use the FortiOS API, you must have an API key.
Host (is required)	Your FortiGate hostname
Name (is required)	Address name
Start IP (is required)	The Start IP which will be used to create the address
End IP (is required)	The End IP which will be used to create the address
Comment	Write a short description about this Address
Color	Color of icon on the GUI.
Allow routing	Enable/disable use of this address in the static route configuration.enable:Enable use of this address in the static route configuration.disable:Disable use of this address in the static route configuration.

Outputs	Description
Status (status)	Success if the API call was executed correctly

Forti/Allow Subnet Address method

Allow Subnet Address.

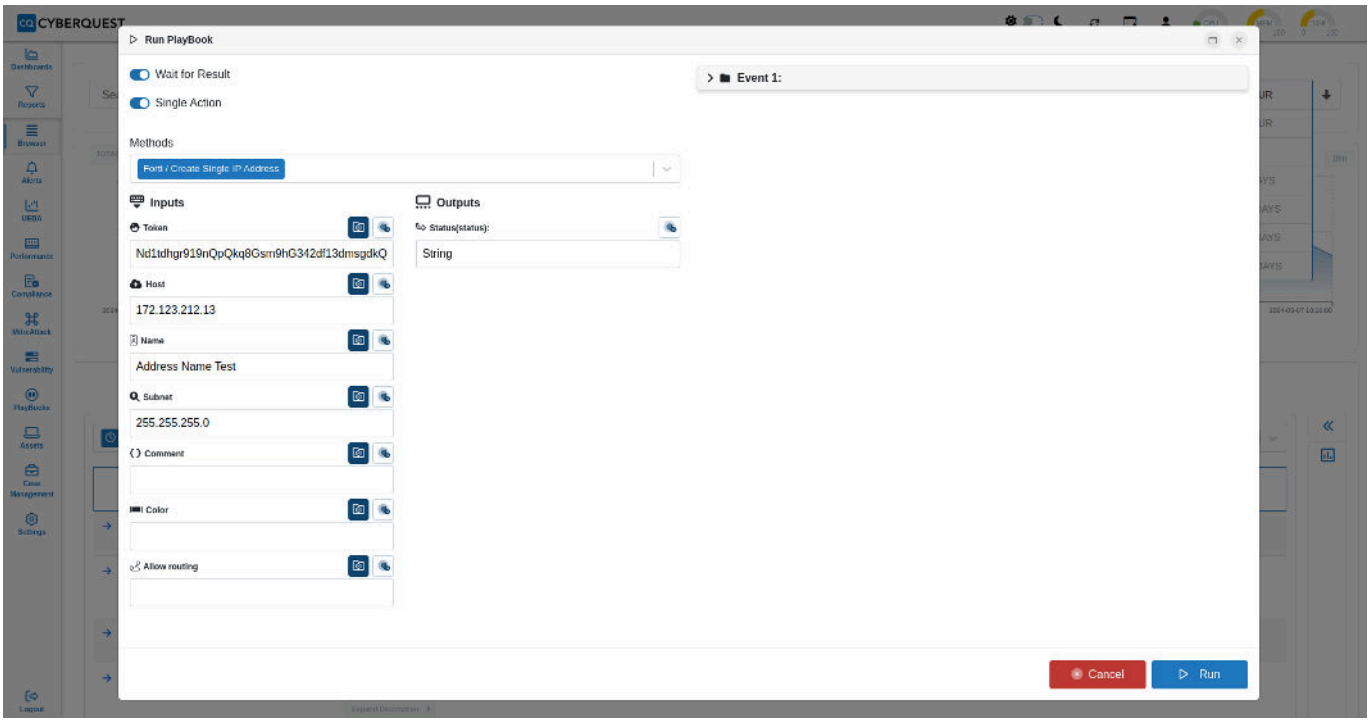


Inputs	Description
Token (is required)	To use the FortiOS API, you must have an API key.
Host (is required)	Your FortiGate hostname
Name (is required)	Address name
IP (is required)	The IP which will be used to create the address
Netmask (is required)	The Netmask which will be used to create the address
Comment	Write a short description about this Address
Color	Color of icon on the GUI.
Allow routing	Enable/disable use of this address in the static route configuration.enable:Enable use of this address in the static route configuration.disable:Disable use of this address in the static route configuration.

Outputs	Description
Status (status)	Success if the API call was executed correctly

Forti/Create Single IP Address method

Create Single IP Address.

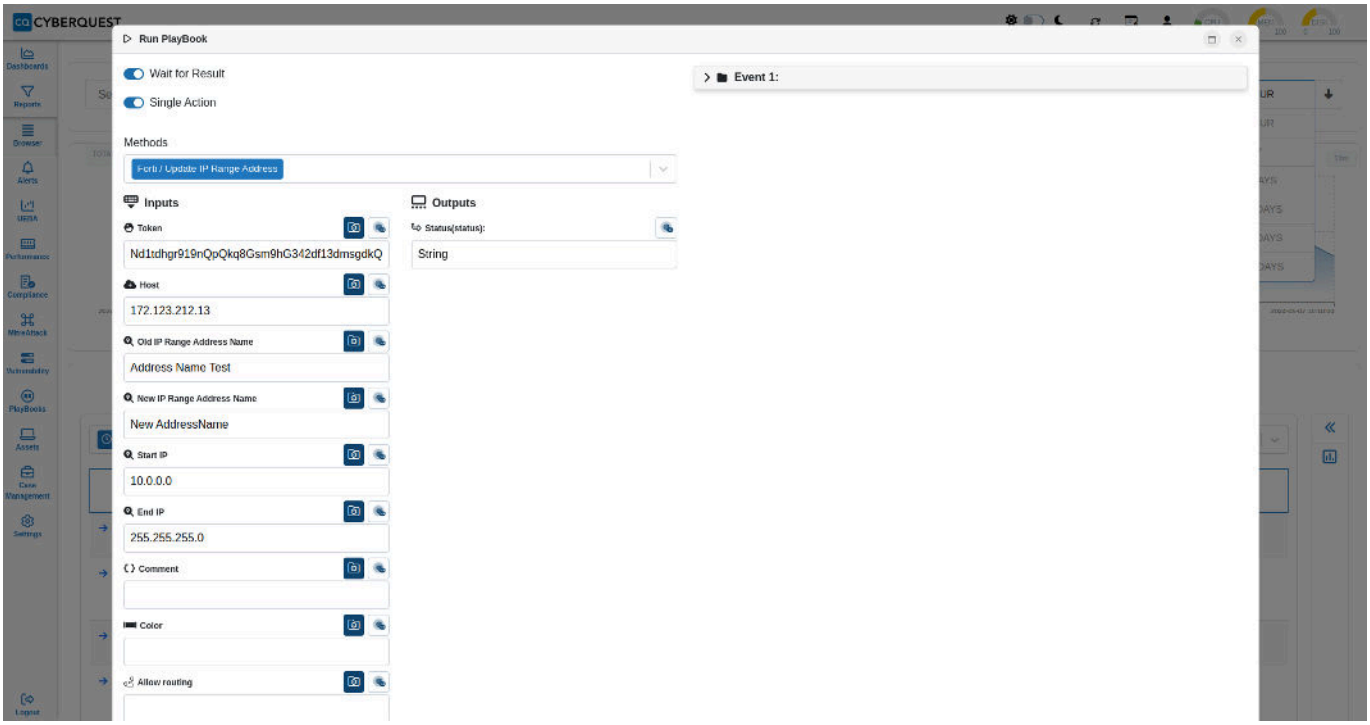


Inputs	Description
Token (is required)	To use the FortiOS API, you must have an API key.
Host (is required)	Your FortiGate hostname
Name (is required)	Address name. To execute with success this API call you need to provide a unique name (which is not already existing in your FortiGate)
Subnet (is required)	The IP which will be used to create the address
Comment	Write a short description about this Address
Color	Color of icon on the GUI.
Allow routing	Enable/disable use of this address in the static route configuration.enable:Enable use of this address in the static route configuration.disable:Disable use of this address in the static route configuration.

Outputs	Description
Status (status)	Success if the API call was executed correctly

Forti/Update IP Range Address method

Update IP Range Address.

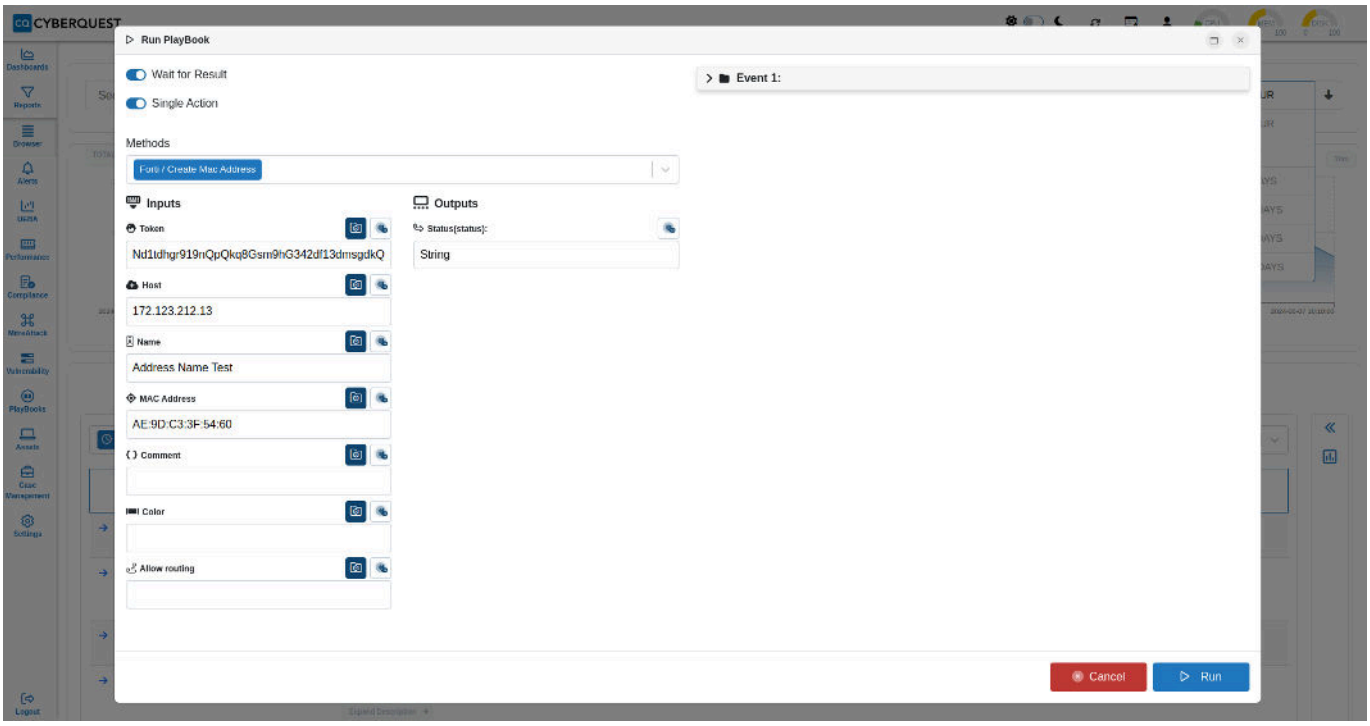


Inputs	Description
Token (is required)	To use the FortiOS API, you must have an API key.
Host (is required)	Your FortiGate hostname
Old IP Range Address Name (is required)	The IP Range Address name which will be changed
New IP Range Address Name (is required)	Address name
Start IP (is required)	First IP address (inclusive) in the range for the address.
End IP (is required)	Final IP address (inclusive) in the range for the address.
Comment	Write a short description about this Address
Color	Color of icon on the GUI.
Allow routing	Enable/disable use of this address in the static route configuration.enable:Enable use of this address in the static route configuration.disable:Disable use of this address in the static route configuration.

Outputs	Description
Status (status)	Success if the API call was executed correctly

Forti/Create Mac Address method

Create an Address which contain MAC Address.

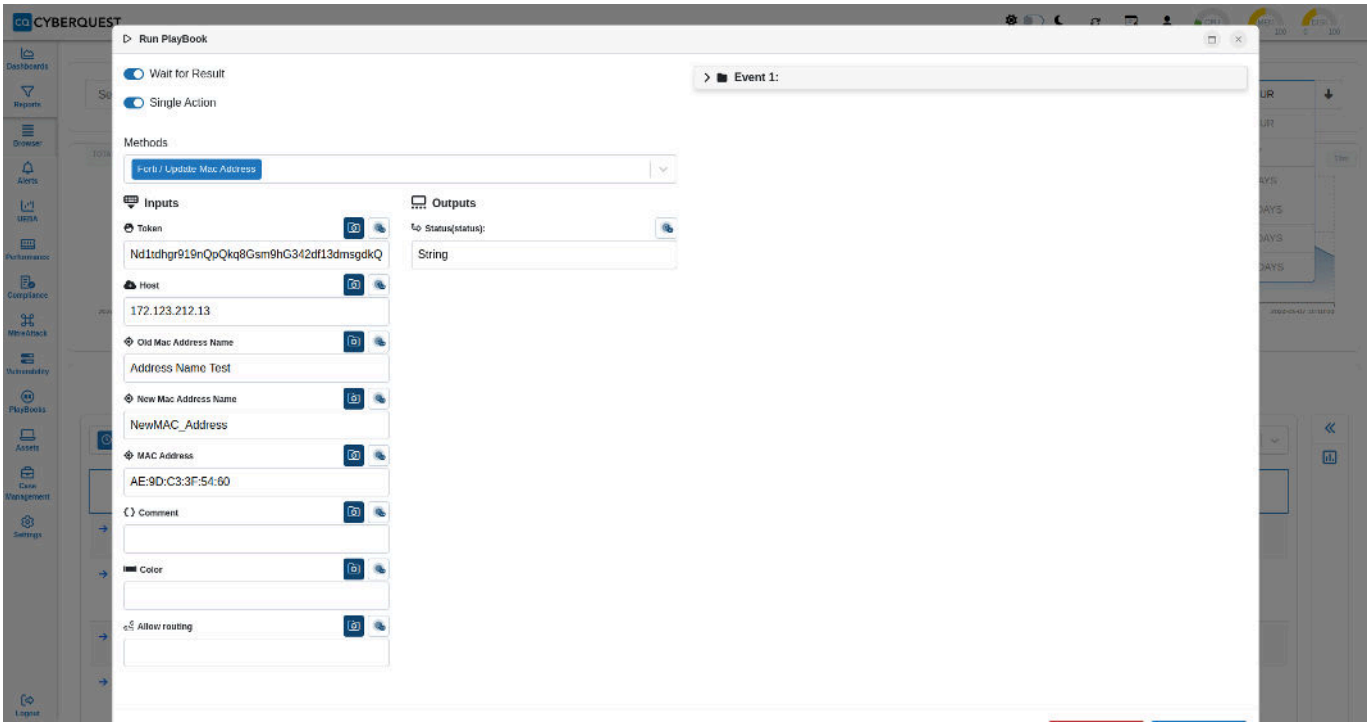


Inputs	Description
Token (is required)	To use the FortiOS API, you must have an API key.
Host (is required)	Your FortiGate hostname
Name (is required)	Address name. To execute with success this API call you need to provide a unique name (which is not already existing in your FortiGate)
MAC Address (is required)	The MAC Address of interest
Comment	Write a short description about this Address
Color	Color of icon on the GUI.
Allow routing	Enable/disable use of this address in the static route configuration.enable:Enable use of this address in the static route configuration.disable:Disable use of this address in the static route configuration.

Outputs	Description
Status (status)	Success if the API call was executed correctly

Forti/Update Mac Address method

Update an Address which contain MAC Address.

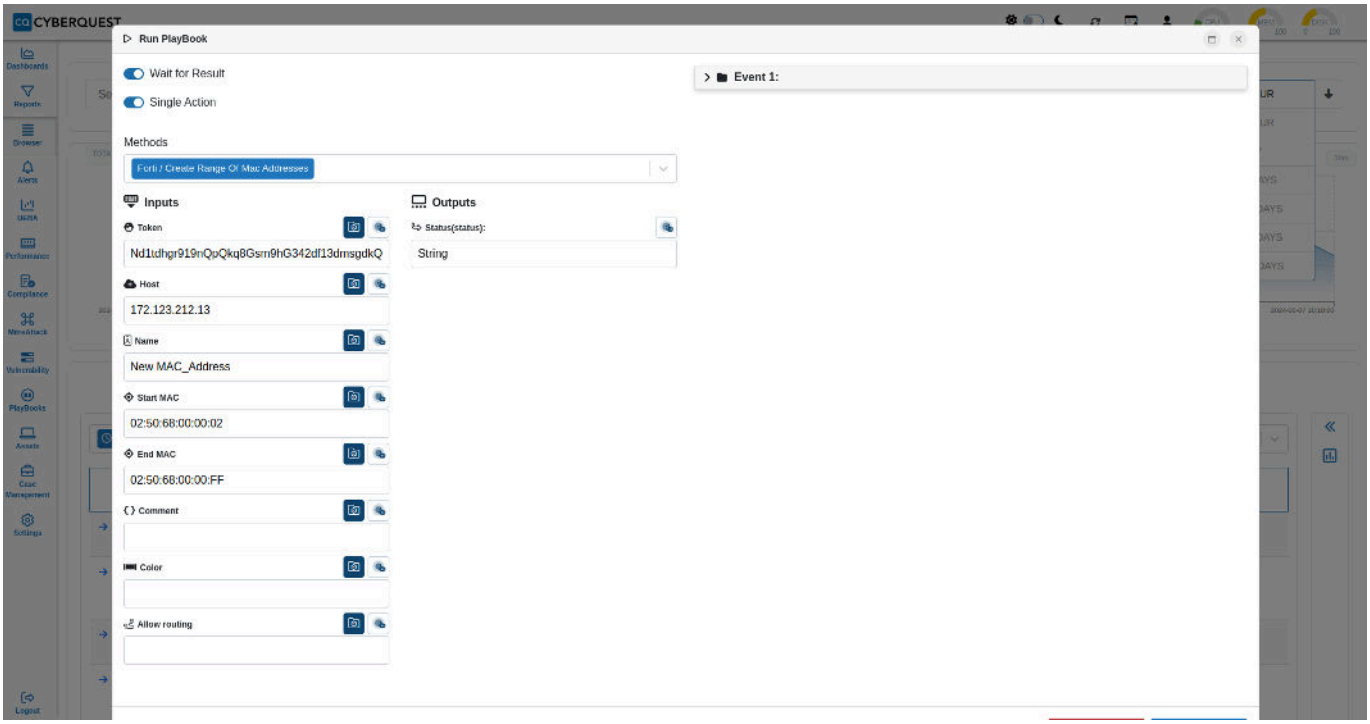


Inputs	Description
Token (is required)	To use the FortiOS API, you must have an API key.
Host (is required)	Your FortiGate hostname
Old Mac Address Name (is required)	The MAC Address name which will be changed
New Mac Address Name (is required)	Address name
MAC Address (is required)	The MAC Address of interest
Comment	Write a short description about this Address
Color	Color of icon on the GUI.
Allow routing	Enable/disable use of this address in the static route configuration.enable:Enable use of this address in the static route configuration.disable:Disable use of this address in the static route configuration.

Outputs	Description
Status (status)	Success if the API call was executed correctly

Forti/Create Range Of Mac Addresses method

Create MAC Range Address.

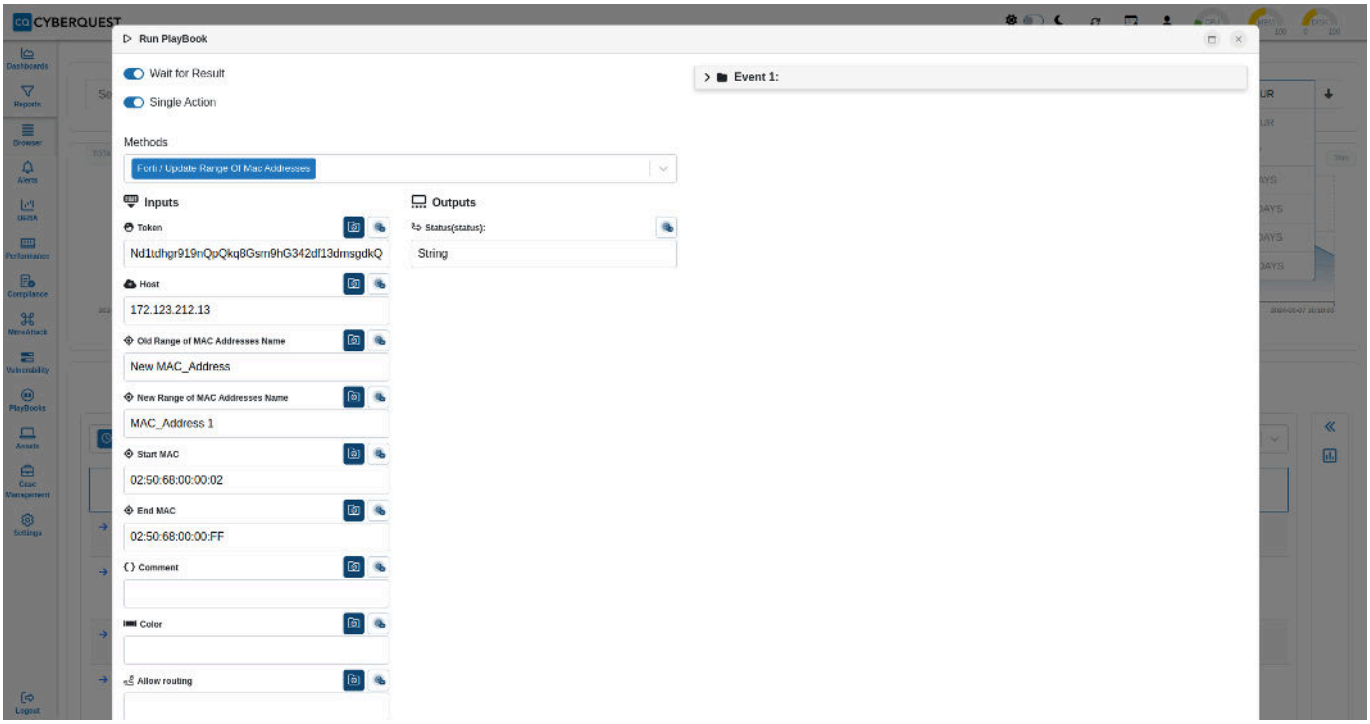


Inputs	Description
Token (is required)	To use the FortiOS API, you must have an API key.
Host (is required)	Your FortiGate hostname
Name (is required)	Address name. To execute with success this API call you need to provide a unique name (which is not already existing in your FortiGate)
Start MAC (is required)	First MAC address in the range.
End MAC (is required)	Last MAC address in the range.
Comment	Write a short description about this Address
Color	Color of icon on the GUI.
Allow routing	Enable/disable use of this address in the static route configuration.enable:Enable use of this address in the static route configuration.disable:Disable use of this address in the static route configuration.

Outputs	Description
Status (status)	Success if the API call was executed correctly

Forti/Update Range Of Mac Addresses method

Update MAC Range Address.

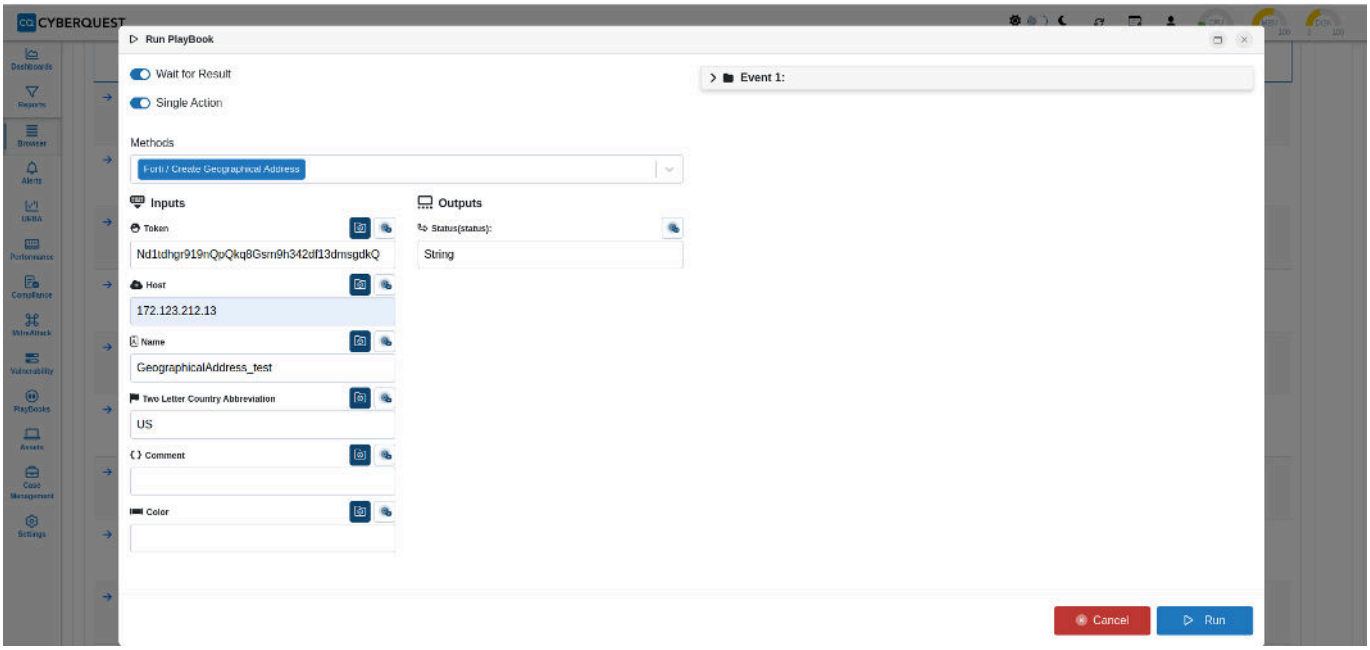


Inputs	Description
Token (is required)	To use the FortiOS API, you must have an API key.
Host (is required)	Your FortiGate hostname
Old Range of MAC Addresses Name (is required)	The MAC Address Range name which will be changed
New Range of MAC Addresses Name (is required)	Address name
Start MAC (is required)	First MAC address in the range.
End MAC (is required)	Last MAC address in the range.
Comment	Write a short description about this Address
Color	Color of icon on the GUI.
Allow routing	Enable/disable use of this address in the static route configuration.enable:Enable use of this address in the static route configuration.disable:Disable use of this address in the static route configuration.

Outputs	Description
Status (status)	Success if the API call was executed correctly

Forti/Create Geographical Address method

Create Geographical Address.

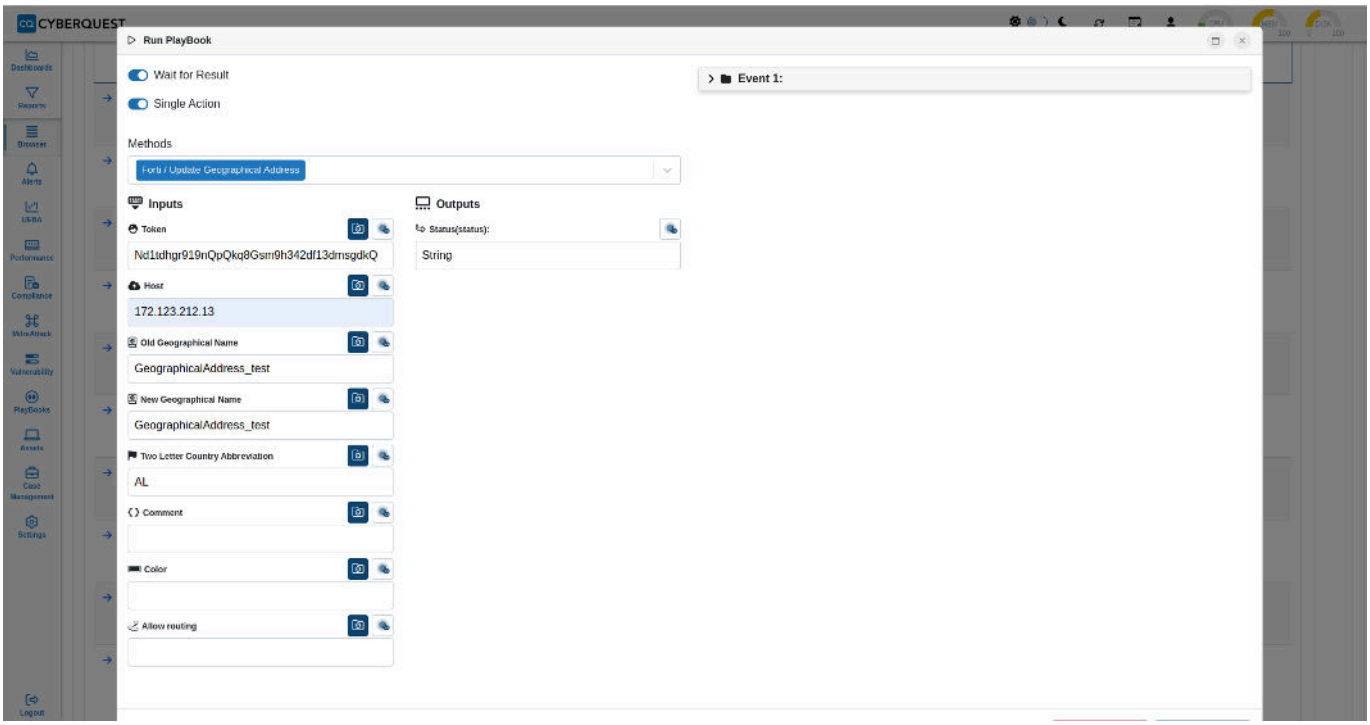


Inputs	Description
Token (is required)	To use the FortiOS API, you must have an API key.
Host (is required)	Your FortiGate hostname
Name (is required)	Address name. To execute with success this API call you need to provide a unique name (which is not already existing in your FortiGate)
Two Letter Country Abbreviation (is required)	The name of the country. Use ISO 3166 notation for countries (ex: US)
Comment	Write a short description about this Address
Color	Color of icon on the GUI.

Outputs	Description
Status (status)	Success if the API call was executed correctly

Forti/Update Geographical Address method

Update Geographical Address.

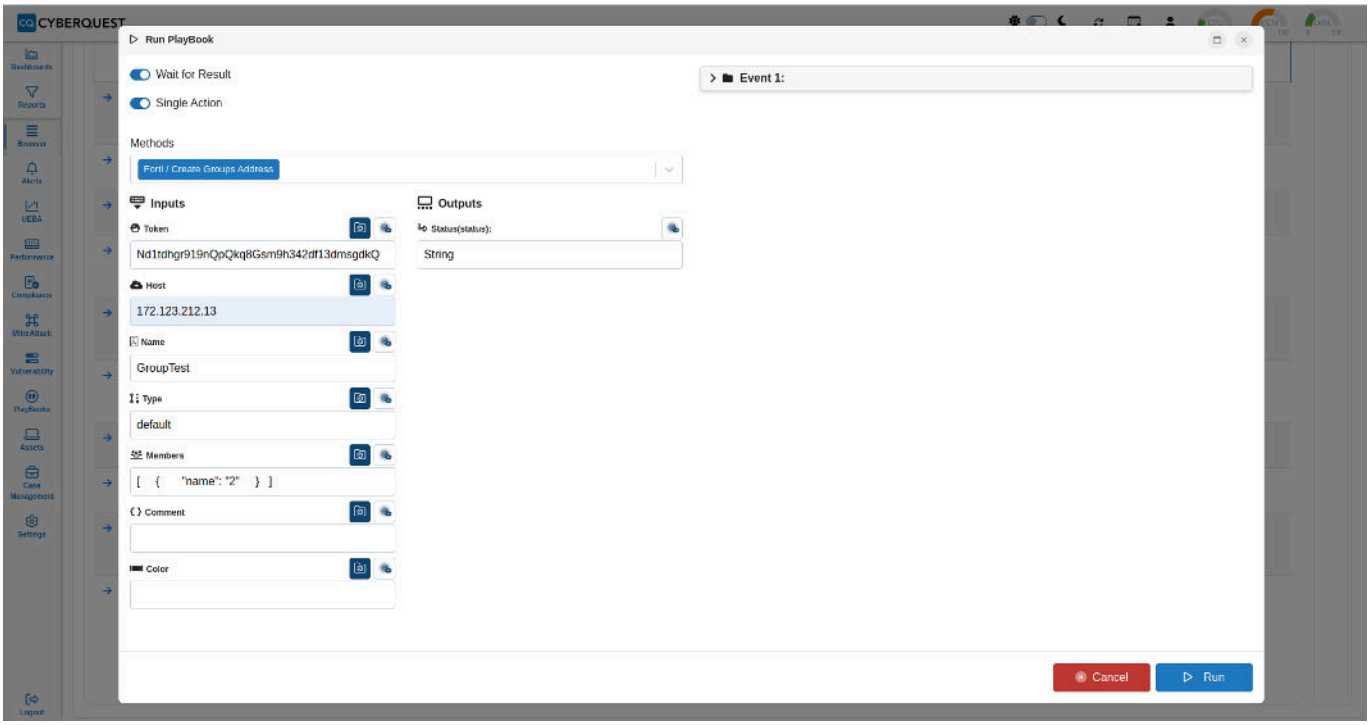


Inputs	Description
Token (is required)	To use the FortiOS API, you must have an API key.
Host (is required)	Your FortiGate hostname
Old Geographical Name (is required)	The Geographical Address name which will be changed
New Geographical Name (is required)	Address name
Two Letter Country Abbreviation (is required)	The name of the country. Use ISO 3166 notation for countries (ex: US)
Comment	Write a short description about this Address
Color	Color of icon on the GUI.
Allow routing	Enable/disable use of this address in the static route configuration.enable:Enable use of this address in the static route configuration.disable:Disable use of this address in the static route configuration.

Outputs	Description
Status (status)	Success if the API call was executed correctly

Forti/Create Groups Address method

Create a Address Group.

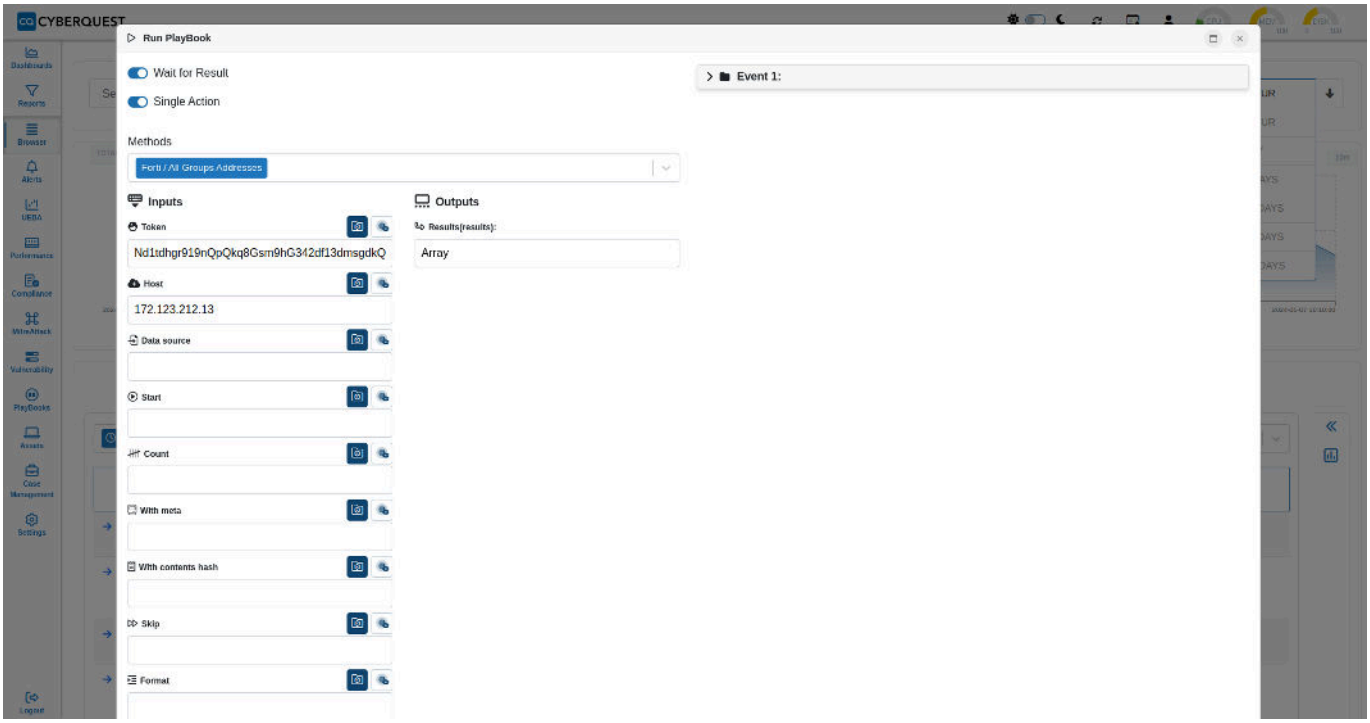


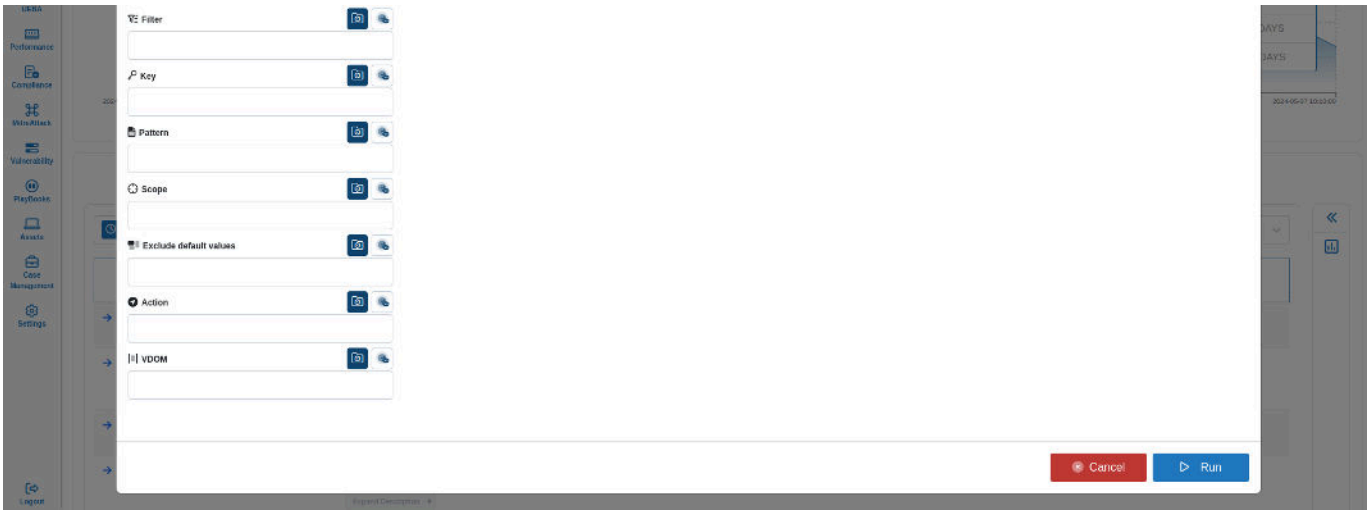
Inputs	Description
Token (is required)	To use the FortiOS API, you must have an API key.
Host (is required)	Your FortiGate hostname
Name (is required)	Address name. To execute with success this API call you need to provide a unique name (which is not already existing in your FortiGate)
Type (is required)	Address group type.default:Default address group type (address may belong to multiple groups).folder:Address folder group (members may not belong to any other group).
Members (is required)	Address objects contained within the group.
Comment	Write a short description about this Address
Color	Color of icon on the GUI.

Outputs	Description
Status (status)	Success if the API call was executed correctly

Forti/All Groups Addresses method

Return all Groups Addresses created.



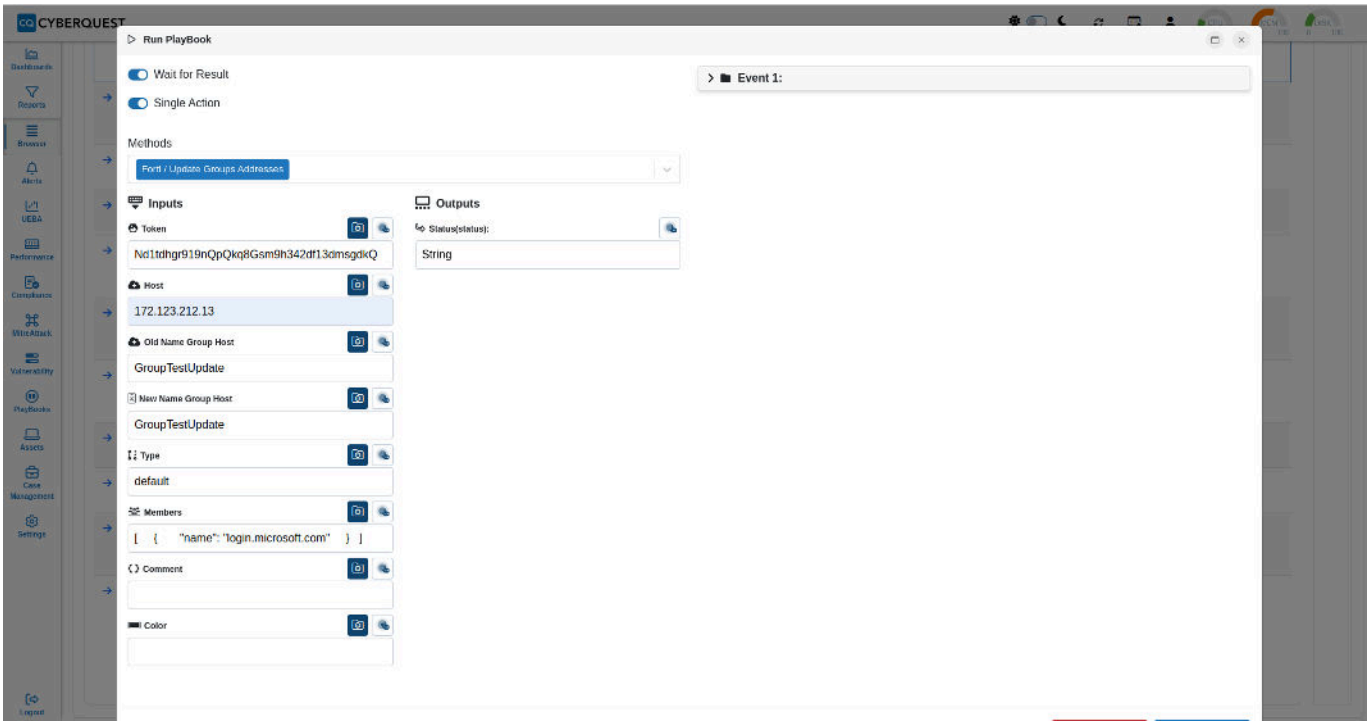


Inputs	Description
Token (is required)	To use the FortiOS API, you must have an API key.
Host (is required)	Your FortiGate hostname
Data source	Enable to include datasource information for each linked object.
Start	Starting entry index.
Count	Maximum number of entries to return.
With meta	Enable to include meta information about each object (type id, references, etc).
With contents hash	Enable to include a checksum of each objects contents.
Skip	Enable to call CLI skip operator to hide skipped properties.
Format	List of property names to include in results, separated by
Filter	Filtering multiple key/value pairsOperator
Key	If present, objects will be filtered on property with this name.
Pattern	If present, objects will be filtered on property with this value.
Scope	Scope [global
Exclude default values	Exclude properties/objects with default value
Action	default: Return the CLI default values for entire CLI tree.meta: Return meta data for a specific object, table, or the entire CLI tree.schema: Return schema for entire CLI tree.
VDOM	Specify the Virtual Domain(s) from which results are returned or changes are applied to. If this parameter is not provided, the management VDOM will be used. If the admin does not have access to the VDOM, a permission error will be returned.The URL parameter is one of:vdom=root (Single VDOM)vdom=vdom1,vdom2 (Multiple VDOMs)vdom=* (All VDOMs)

Outputs	Description
Results (results)	The results of the API call

Forti/Update Groups Addresses method

Update an Address Group.

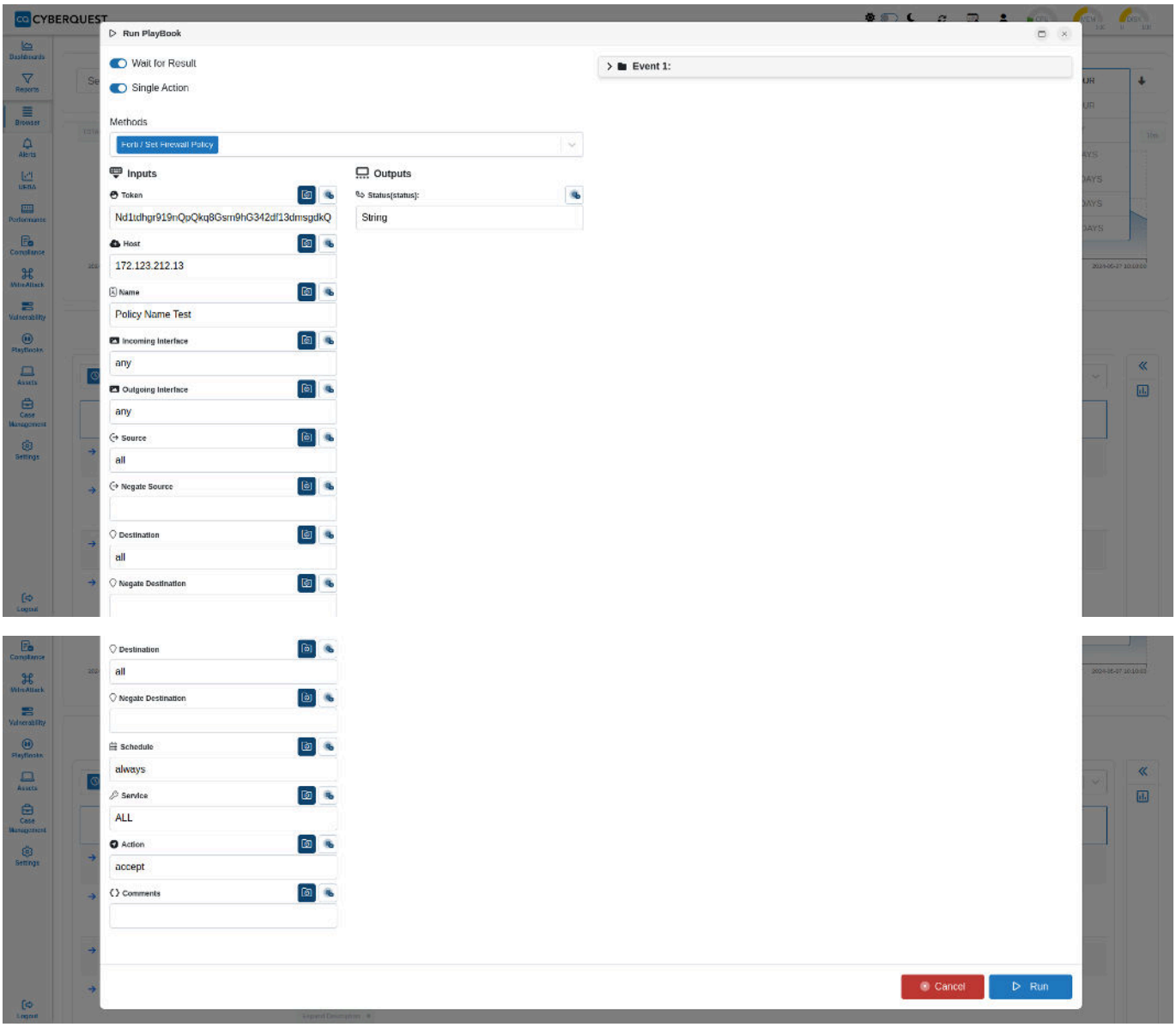


Inputs	Description
Token (is required)	To use the FortiOS API, you must have an API key.
Host (is required)	Your FortiGate hostname
Old Name Group Host (is required)	Address Name what you want to update
New Name Group Host (is required)	Address name
Type (is required)	Address group type.default:Default address group type (address may belong to multiple groups).folder:Address folder group (members may not belong to any other group).
Member	Address objects contained within the group.
Comment	Write a short description about this Address
Color	Color of icon on the GUI.

Outputs	Description
Status (status)	Success if the API call was executed correctly

Forti/Set Firewall Policy method

Set Firewall Policy.

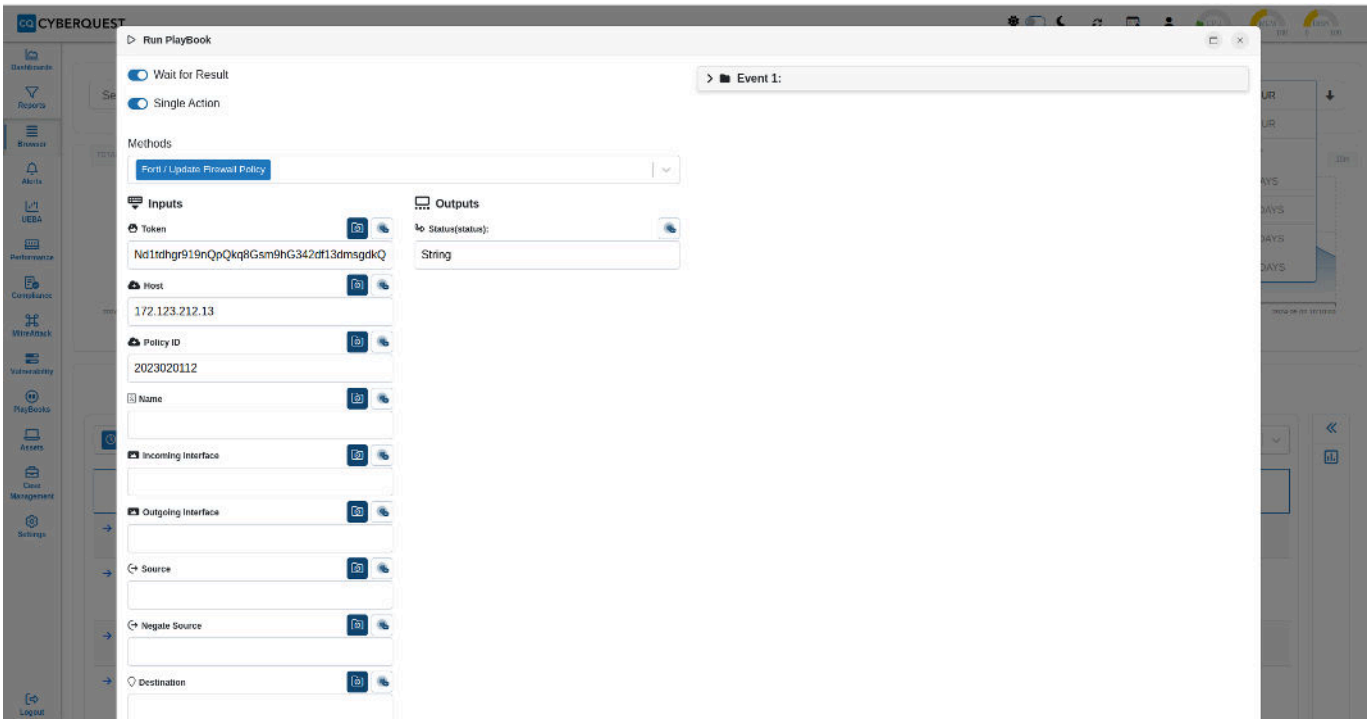

CYBERQUEST
Run PlayBook
Wait for Result
Single Action
Event 1:
Methods
Forti / Set Firewall Policy
Inputs
Outputs
Token
Nd1tdhgr919nQpQkq8Gsrn9hG342df13dmsgdkQ
Status(status):
String
Host
172.123.212.13
Name
Policy Name Test
Incoming Interface
any
Outgoing Interface
any
Source
all
Negate Source
Destination
all
Negate Destination
Destination
all
Negate Destination
Schedule
always
Service
ALL
Action
accept
Comments
Cancel
Run

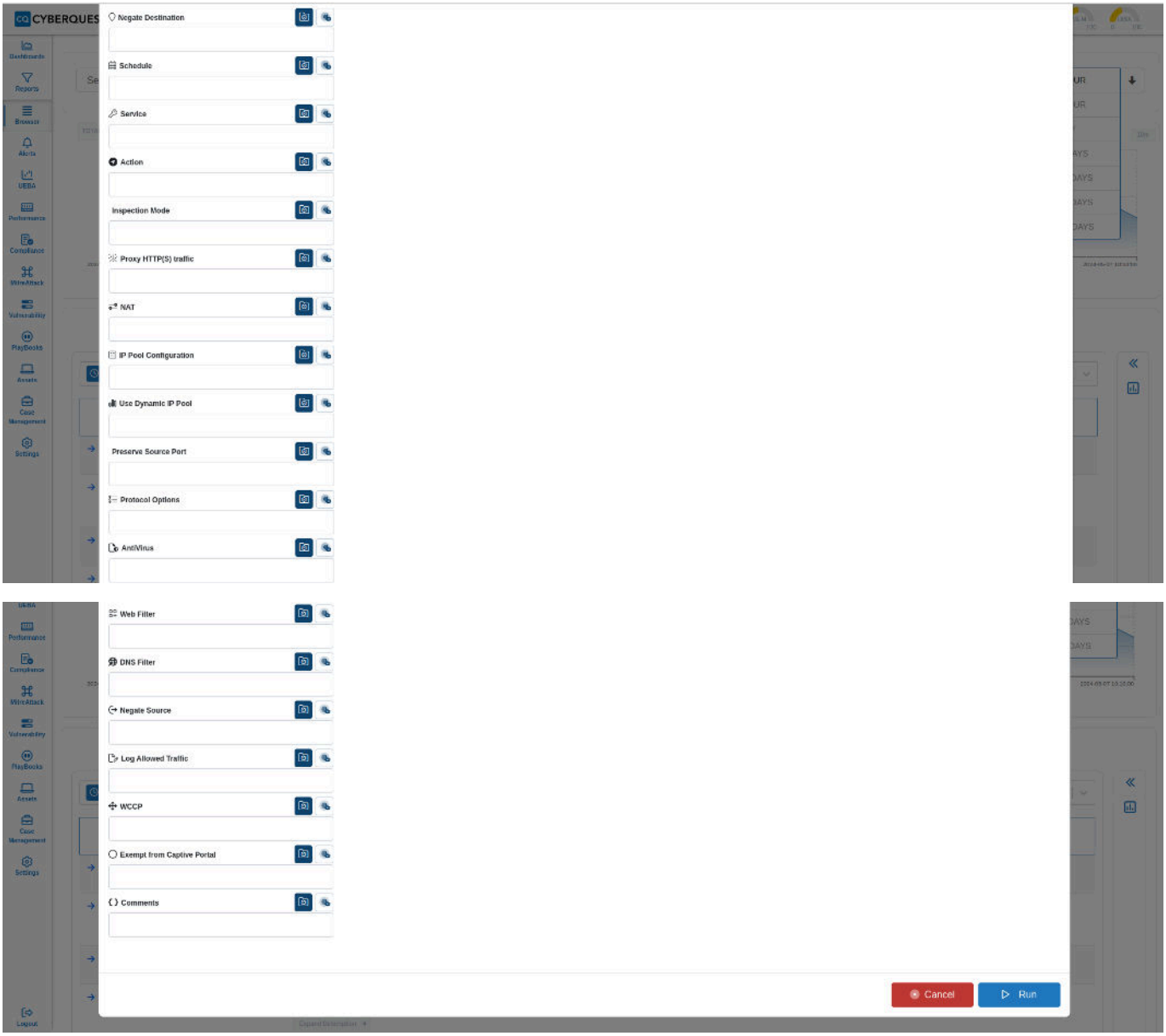
Inputs	Description
Token (is required)	To use the FortiOS API, you must have an API key.
Host (is required)	Your FortiGate hostname
Name (is required)	Policy Name
Incoming Interface (is required)	Incoming (ingress) interface.
Outgoing Interface (is required)	Outgoing (egress) interface.
Source (is required)	Source IPv4 address and address group names.
Negate Source	specifies what the source address must NOT be.enable:Enable source address negate.disable:Disable source address negate.
Destination (is required)	Destination IPv4 address and address group names.
Negate Destination	specifies what the destination address must NOT be.enable:Enable destination address negate.disable:Disable destination address negate.
Schedule (is required)	Schedule name.
Service (is required)	Service and service group names.
Action (is required)	Policy action (accept/deny/ipsec).accept:Allows session that match the firewall policy.deny:Blocks sessions that match the firewall policy.ipsec:Firewall policy becomes a policy-based IPsec VPN policy.
Comments	Comment

Outputs	Description
Status (status)	Success if the API call was executed correctly

Forti/Update Firewall Policy method

Update Firewall Policy.



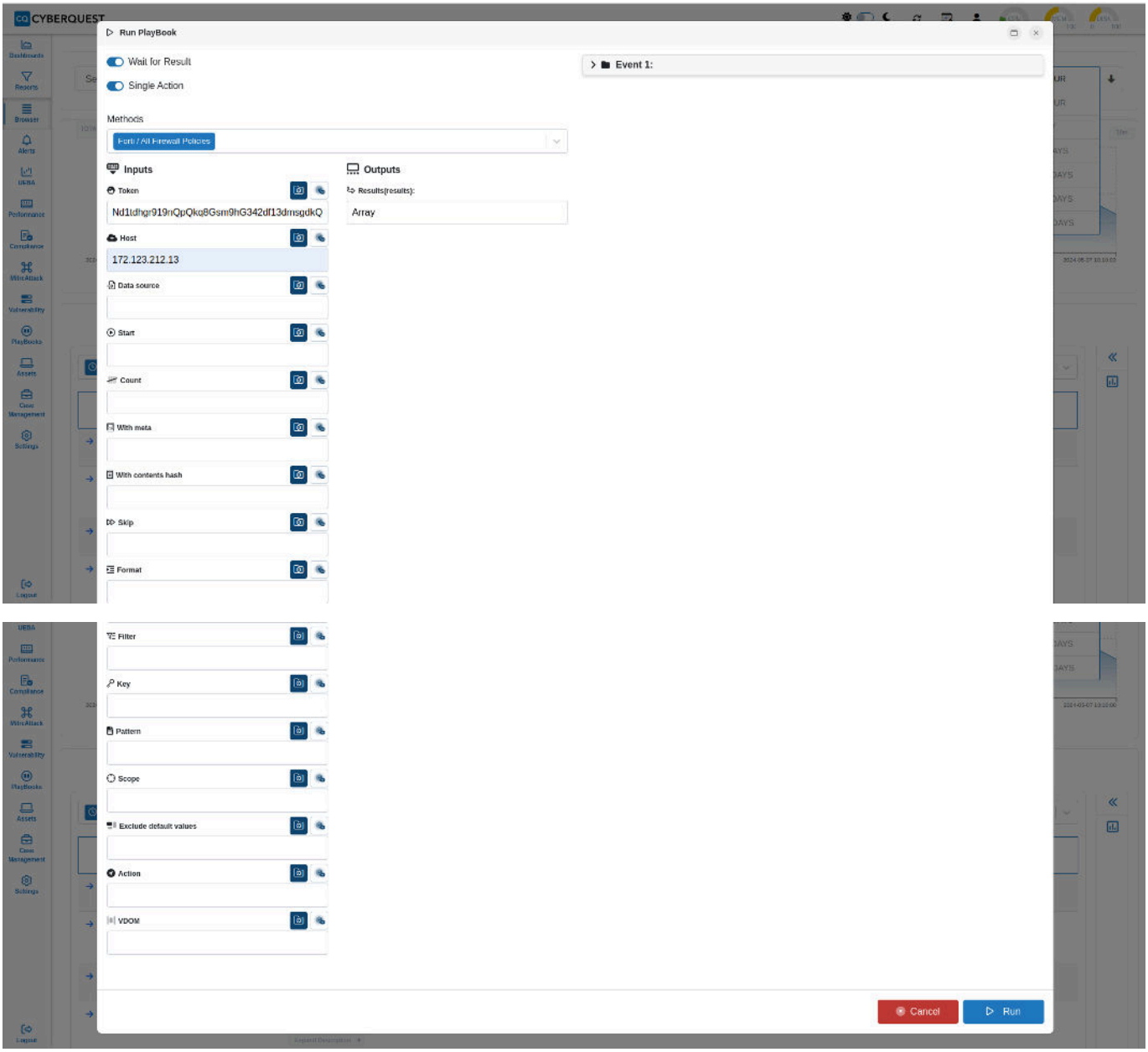

Negate Destination
Schedule
Service
Action
Inspection Mode
Proxy HTTP(S) traffic
NAT
IP Pool Configuration
Use Dynamic IP Pool
Preserve Source Port
Protocol Options
AntiVirus
Web Filter
DNS Filter
Negate Source
Log Allowed Traffic
WCCP
Exempt from Captive Portal
Comments
Cancel
Run

Inputs	Description
Token (is required)	To use the FortiOS API, you must have an API key.
Host (is required)	Your FortiGate hostname
Policy ID (is required)	The policy ID which will be used to identify the policy
Name	Policy Name
Incoming Interface	Incoming (ingress) interface.
Outgoing Interface	Outgoing (egress) interface.
Source	Source IPv4 address and address group names.
Negate Source	specifies what the source address must NOT be.enable:Enable source address negate.disable:Disable source address negate.
Destination	Destination IPv4 address and address group names.
Negate Destination	specifies what the destination address must NOT be.enable:Enable destination address negate.disable:Disable destination address negate.
Schedule	Schedule name.
Service	Service and service group names.
Action	Policy action (accept/deny/ipsec).accept:Allows session that match the firewall policy.deny:Blocks sessions that match the firewall policy.ipsec:Firewall policy becomes a policy-based IPsec VPN policy.
Inspection Mode	Policy inspection mode (Flow/proxy). Default is Flow mode.proxy:Proxy based inspection.flow:Flow based inspection. If selected the Proxy based you must disable or enable Proxy HTTP(S) traffic
Proxy HTTP(S) traffic	Redirect HTTP(S) traffic to matching transparent web proxy policy.enable:Enable HTTP(S) policy redirect.disable:Disable HTTP(S) policy redirect
NAT	Enable/disable source NAT.enable:Enable setting.disable:Disable setting.
IP Pool Configuration	Enable to use IP Pools for source NAT.enable:Enable setting.disable:Disable setting.
Use Dynamic IP Pool	IP Pool names. IF IP Pool configuration is enabled this parameter must pe completed
Preserve Source Port	Enable to prevent source NAT from changing a sessions source port.enable:Enable setting.disable:Disable setting.
Protocol Options	Name of an existing Protocol options profile. If you dont have anything declared use default
AntiVirus	Name of an existing Antivirus profile.
Web Filter	Name of an existing Web filter profile.
DNS Filter	Name of an existing DNS filter profile.
Negate Source	specifies what the source address must NOT be.enable:Enable source address negate.disable:Disable source address negate.
Log Allowed Traffic	Enable or disable logging. Log all sessions or security profile sessions.all:Log all sessions accepted or denied by this policy.utm:Log traffic that has a security profile applied to it.disable:Disable all logging for this policy.
WCCP	Enable/disable forwarding traffic matching this policy to a configured WCCP server.enable:Enable WCCP setting.disable:Disable WCCP setting
Exempt from Captive Portal	Enable to exempt some users from the captive portal.enable:Enable exemption of captive portal.disable:Disable exemption of captive portal.
Comments	Comment

Outputs	Description
Status (status)	Success if the API call was executed correctly

Forti/All Firewall Policies method

Return all Policies created.

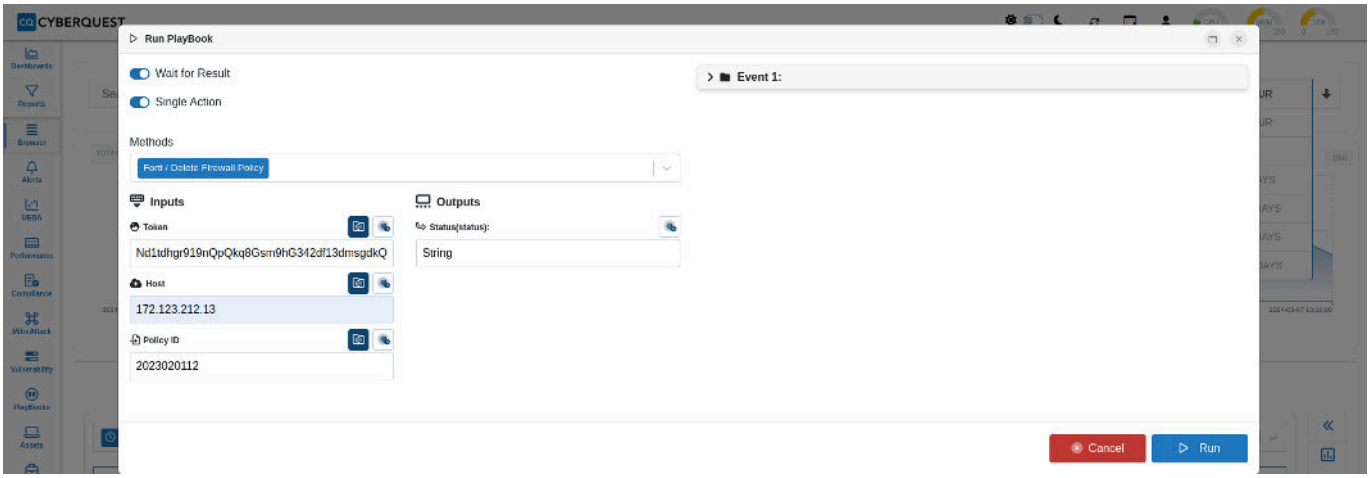


Inputs	Description
Token (is required)	To use the FortiOS API, you must have an API key.
Host (is required)	Your FortiGate hostname
Data source	Enable to include datasource information for each linked object.
Start	Starting entry index.
Count	Maximum number of entries to return.
With meta	Enable to include meta information about each object (type id, references, etc).
With contents hash	Enable to include a checksum of each objects contents.
Skip	Enable to call CLI skip operator to hide skipped properties.
Format	List of property names to include in results, separated by
Filter	Filtering multiple key/value pairsOperator
Key	If present, objects will be filtered on property with this name.
Pattern	If present, objects will be filtered on property with this value.
Scope	Scope [global
Exclude default values	Exclude properties/objects with default value
Action	default: Return the CLI default values for entire CLI tree.meta: Return meta data for a specific object, table, or the entire CLI tree.schema: Return schema for entire CLI tree.
VDOM	Specify the Virtual Domain(s) from which results are returned or changes are applied to. If this parameter is not provided, the management VDOM will be used. If the admin does not have access to the VDOM, a permission error will be returned.The URL parameter is one of:vdom=root (Single VDOM)vdom=vdom1,vdom2 (Multiple VDOMs)vdom=* (All VDOMs)

Outputs	Description
Results (results)	The results of the API call

Forti/Delete Firewall Policy method

Delete a specific Policy.

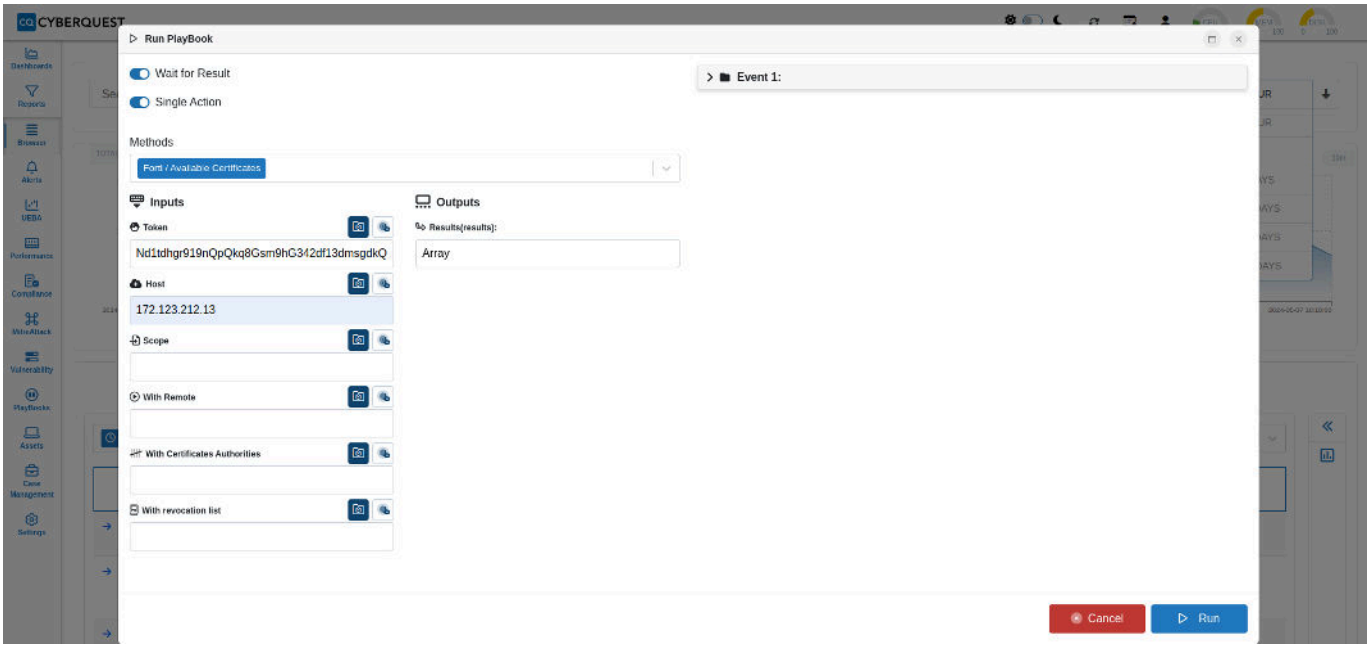


Inputs	Description
Token (is required)	To use the FortiOS API, you must have an API key.
Host (is required)	Your FortiGate hostname
Policy ID (is required)	The ID of Policy you want to delete

Outputs	Description
Status (status)	Success if the API call was executed correctly

Forti/Available Certificates method

Get Available Certificates.

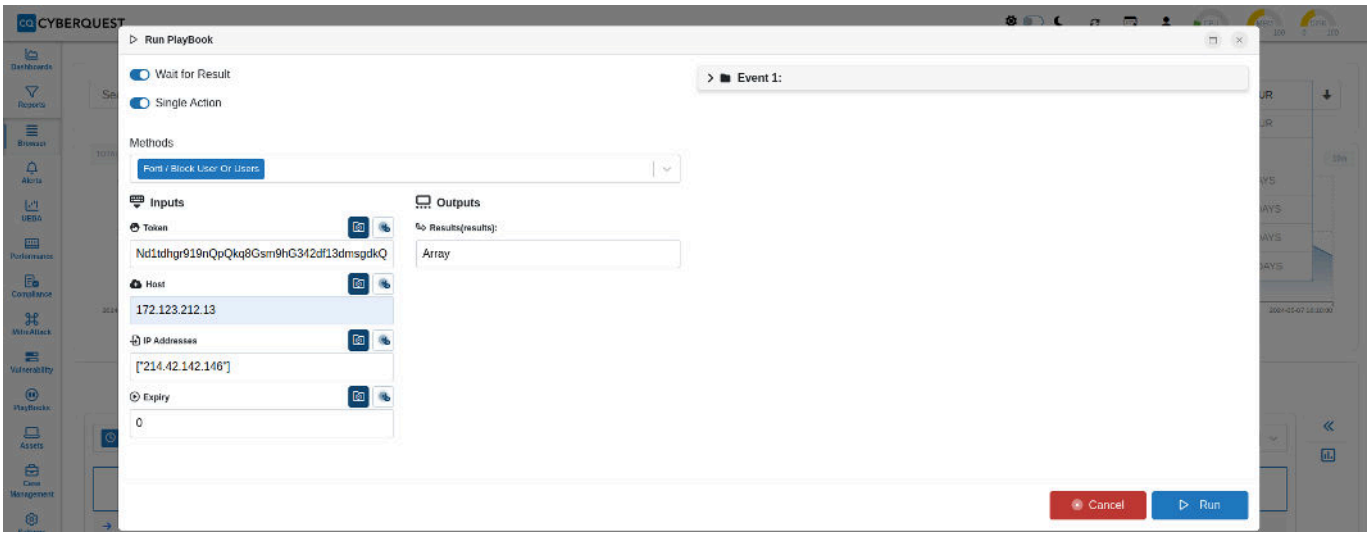


Inputs	Description
Token (is required)	To use the FortiOS API, you must have an API key.
Host (is required)	Your FortiGate hostname
Scope	Scope of certificate [vdom*
With Remote	Include remote certificates.
With Certificates Authorities	Include certificate authorities.
With revocation list	nclude certificate revocation lists.

Outputs	Description
Results (results)	The results of the API call

Forti/Block User Or Users method

Immediately add one or more users to the banned list.

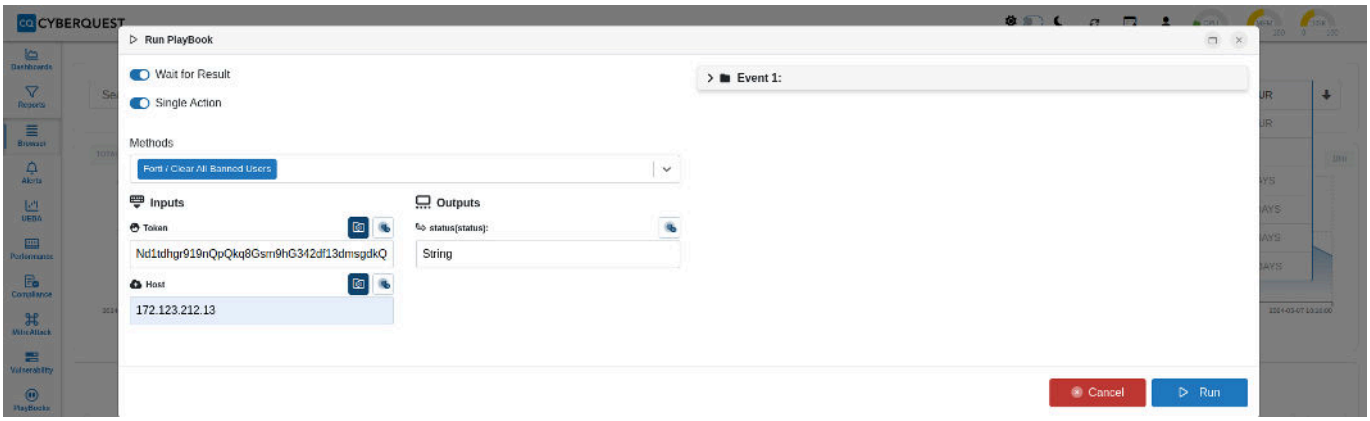


Inputs	Description
Token (is required)	To use the FortiOS API, you must have an API key.
Host (is required)	Your FortiGate hostname
IP Addresses (is required)	List of IP Addresses to ban. IPv4 and IPv6 addresses are allowed
Expiry (is required)	Time until expiry in seconds. 0 for indefinite ban.

Outputs	Description
Results (results)	The results of the API call

Forti/Clear All Banned Users method

Immediately clear all banned users.

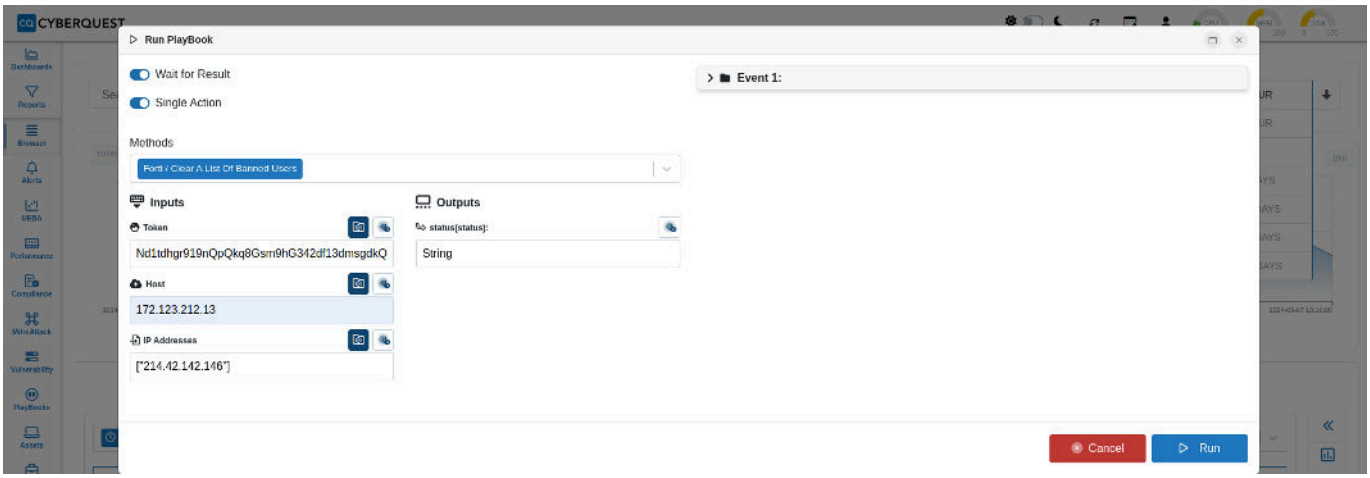


Inputs	Description
Token (is required)	To use the FortiOS API, you must have an API key.
Host (is required)	Your FortiGate hostname

Outputs	Description
status (status)	Success if the API call was executed correctly

Forti/Clear A List Of Banned Users method

Immediately clear a list of specific banned users by IP.

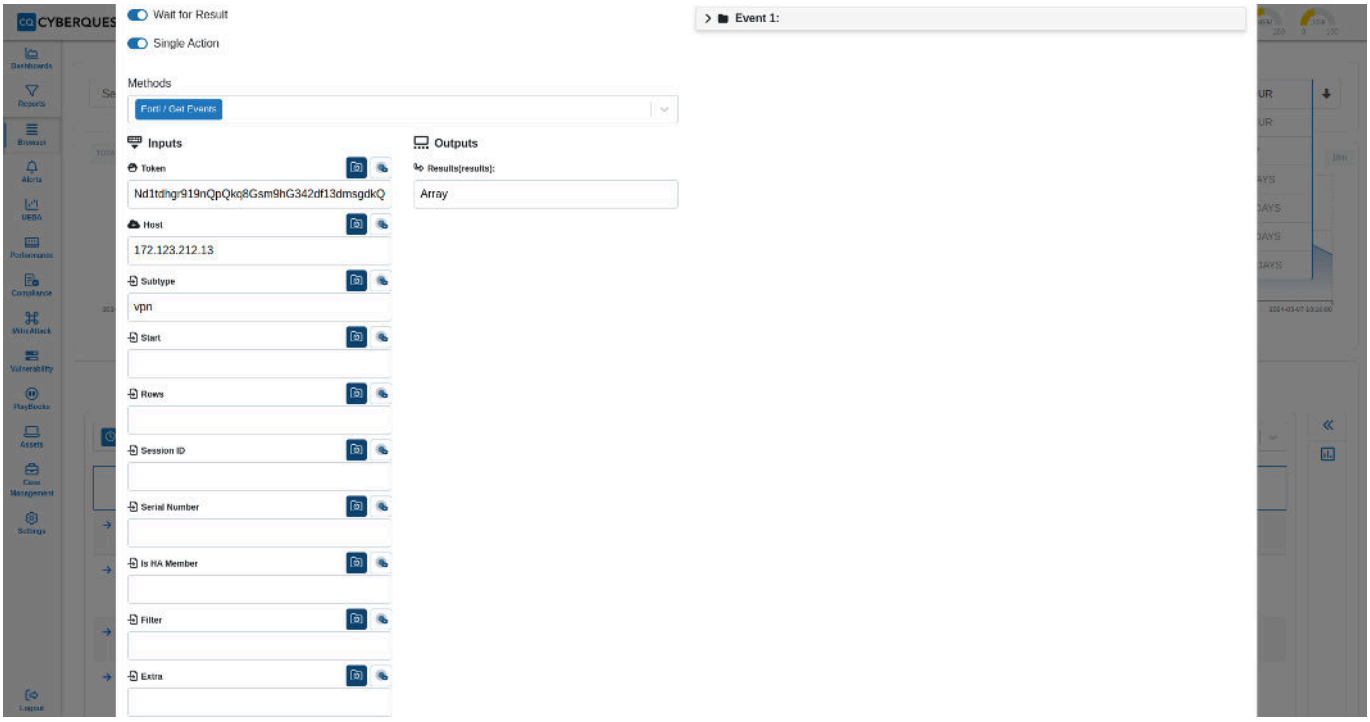


Inputs	Description
Token (is required)	To use the FortiOS API, you must have an API key.
Host (is required)	Your FortiGate hostname
IP Addresses (is required)	List of banned user IPs to clear. IPv4 and IPv6 addresses are allowed.

Outputs	Description
status (status)	Success if the API call was executed correctly

Forti/Get Events method

Log Data.

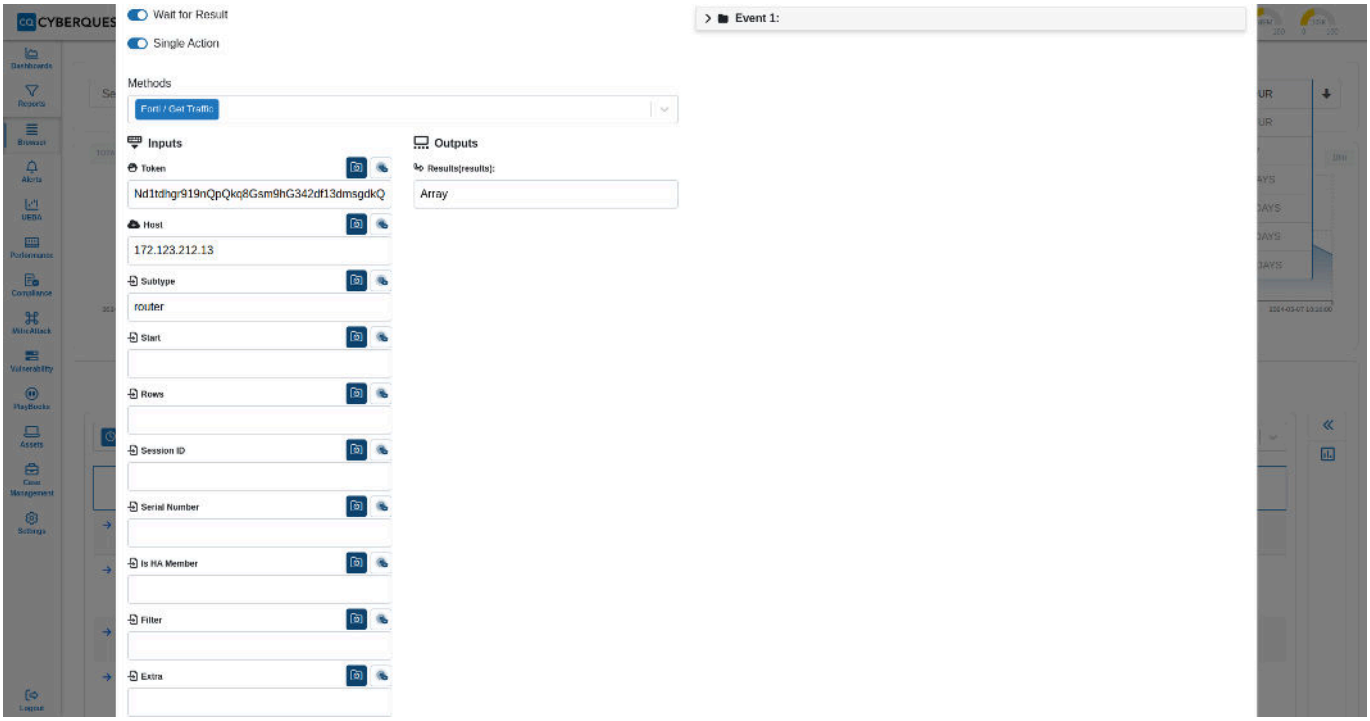


Inputs	Description
Token (is required)	To use the FortiOS API, you must have an API key.
Host (is required)	Your FortiGate hostname
Subtype (is required)	Select the subtype for the Event log categoryAvailable values : vpn, user, router, wireless, wad, endpoint, ha, compliance-check, security-rating, fortiextender, connector, system
Start	Row number for the first row to return
Rows	Number of rows to return.
Session ID	Provide a session_id to continue getting data for that request.
Serial Number	Retrieve log from the specified device.
Is HA Member	Is the specified device an HA member.
Filter	Filtering multiple key/value pairsOperator
Extra	Flag(s) for extra data to be included [reverse_lookup

Outputs	Description
Results (results)	The results of the API call

Forti/Get Traffic method

Get Log Traffic Data.

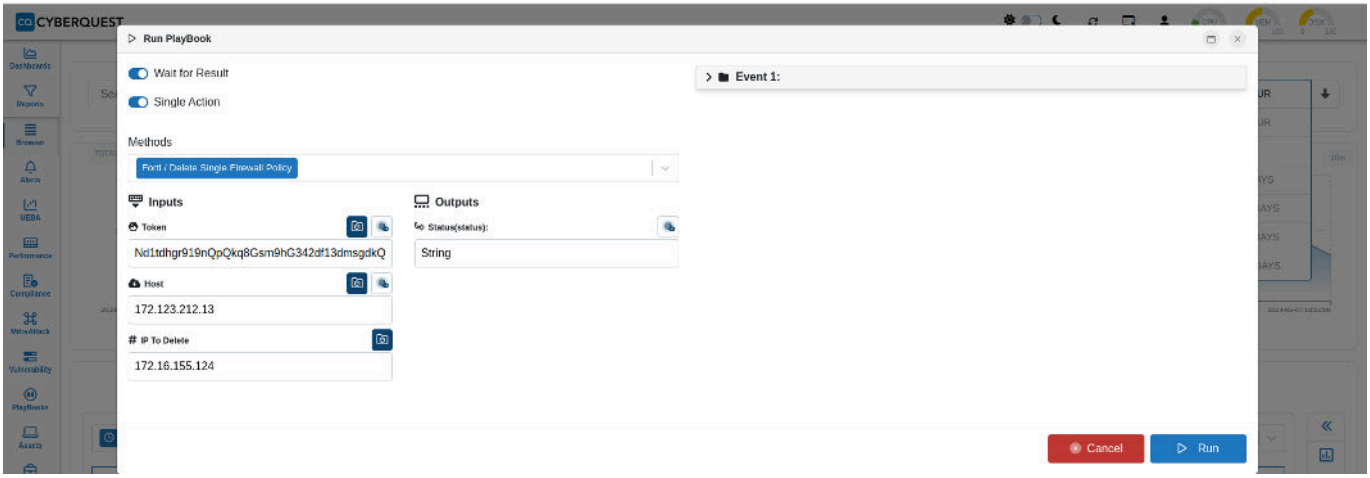


Inputs	Description
Token (is required)	To use the FortiOS API, you must have an API key.
Host (is required)	Your FortiGate hostname
Subtype (is required)	Select the subtype for the Traffic log category. Available values: forward, local, multicast, sniffer, fortiview, threat
Start	Row number for the first row to return
Rows	Number of rows to return.
Session ID	Provide a session_id to continue getting data for that request.
Serial Number	Retrieve log from the specified device.
Is HA Member	Is the specified device an HA member.
Filter	Filtering multiple key/value pairsOperator
Extra	Flag(s) for extra data to be included [reverse_lookup

Outputs	Description
Results (results)	The results of the API call

Forti/Delete Single Firewall Policy method

Delete a Single Firewall Policy.



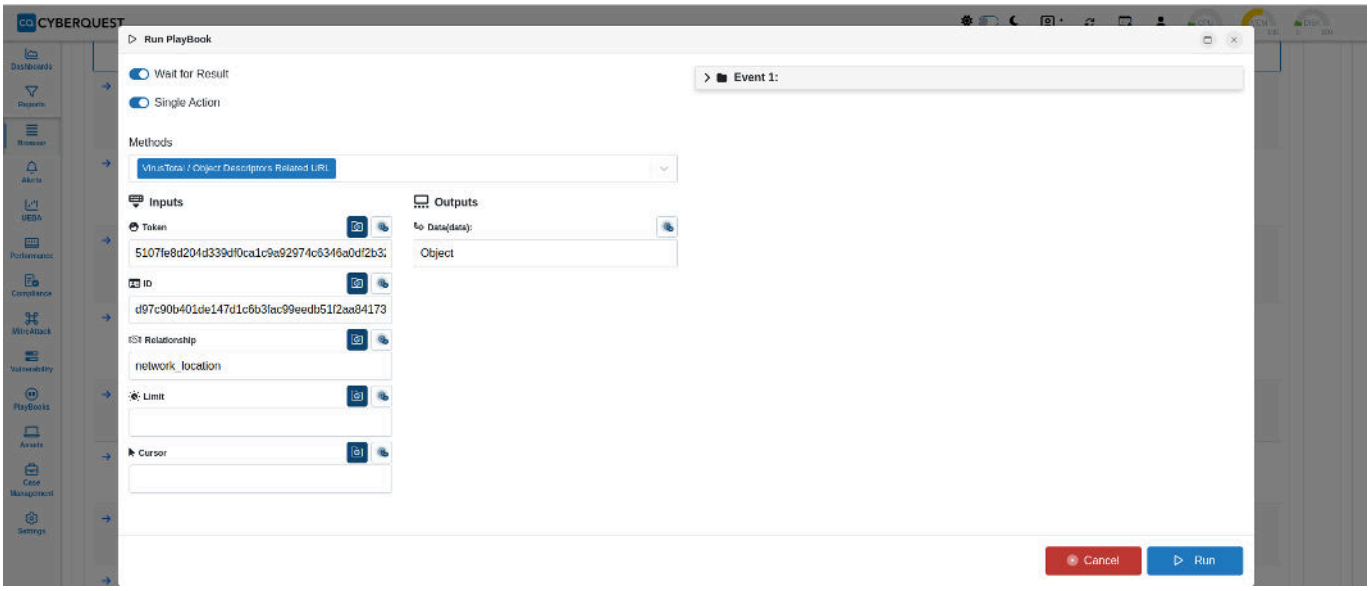
Inputs	Description
Token (is required)	To use the FortiOS API, you must have an API key.
Host (is required)	Your FortiGate hostname
IP To Delete (is required)	The name of the policy you want to delete

Outputs	Description
Status (status)	Success if the API call was executed correctly

VirusTotal

VirusTotal/Object Descriptors Related URL method

Returns just the related objects IDs (and context attributes, if any).

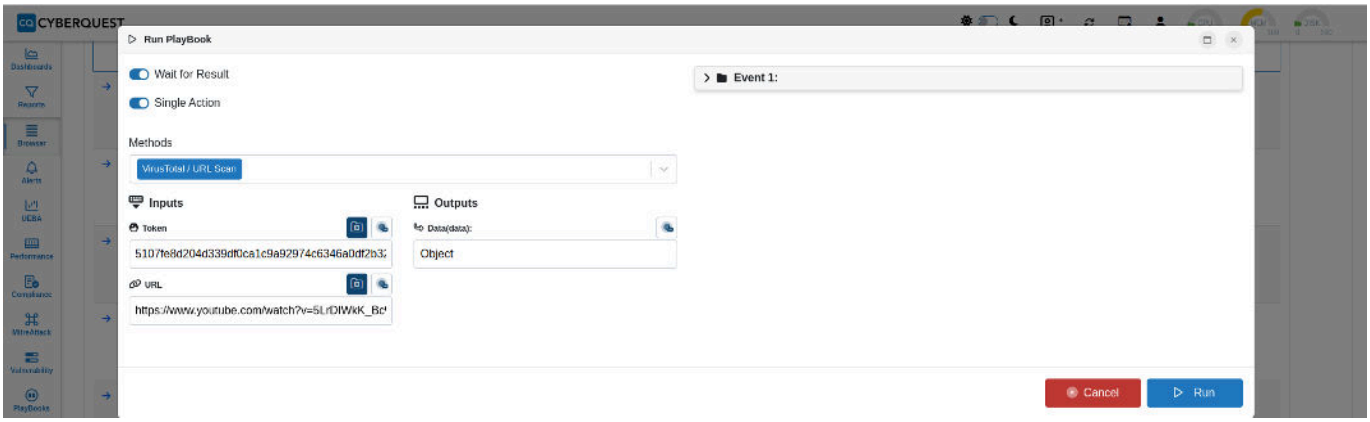


Inputs	Description
Token (is required)	To use the VirusTotal API, you must have an API key.
ID (is required)	The ID given by VirusTotal for investigation of URL
Relationship (is required)	Relationship name
Limit	Maximum number of related objects to retrieve
Cursor	Continuation cursor

Outputs	Description
Data (data)	The results of the API call

VirusTotal/URL Scan method

Perform a URL scan.

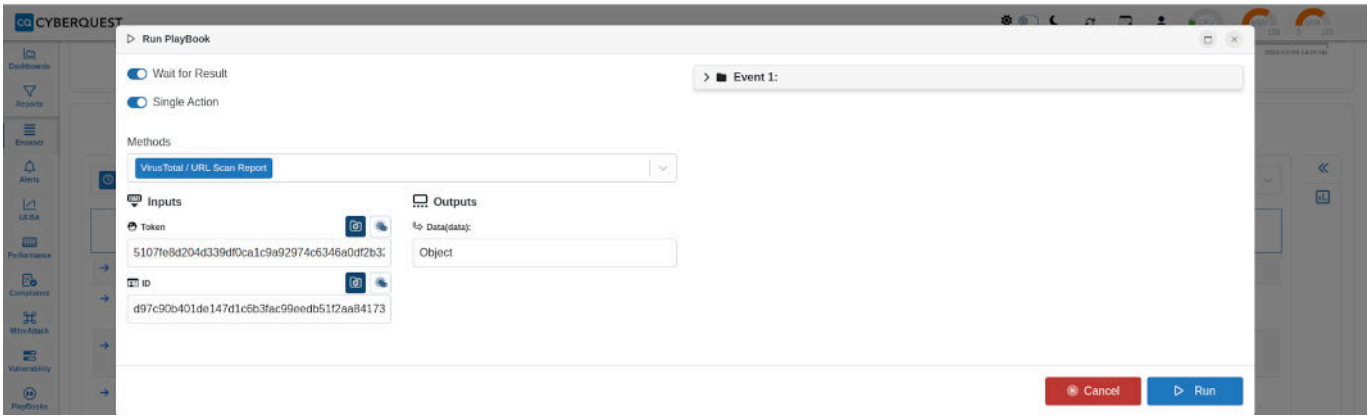


Inputs	Description
Token (is required)	To use the VirusTotal API, you must have an API key.
URL (is required)	URL to scan

Outputs	Description
Data (data)	The results of the API call

VirusTotal/URL Scan Report method

Receive URL analysis report.

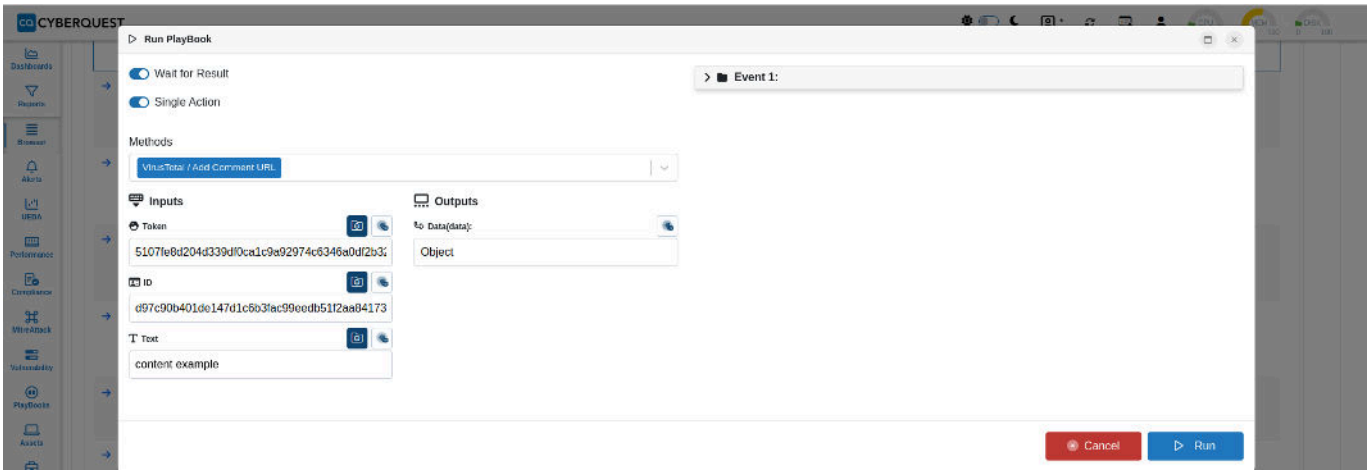


Inputs	Description
Token (is required)	To use the VirusTotal API, you must have an API key.
ID (is required)	The ID given by VirusTotal for investigation URL

Outputs	Description
Data (data)	The results of the API call

VirusTotal/Add Comment URL method

With this endpoint you can post a comment for a given URL.

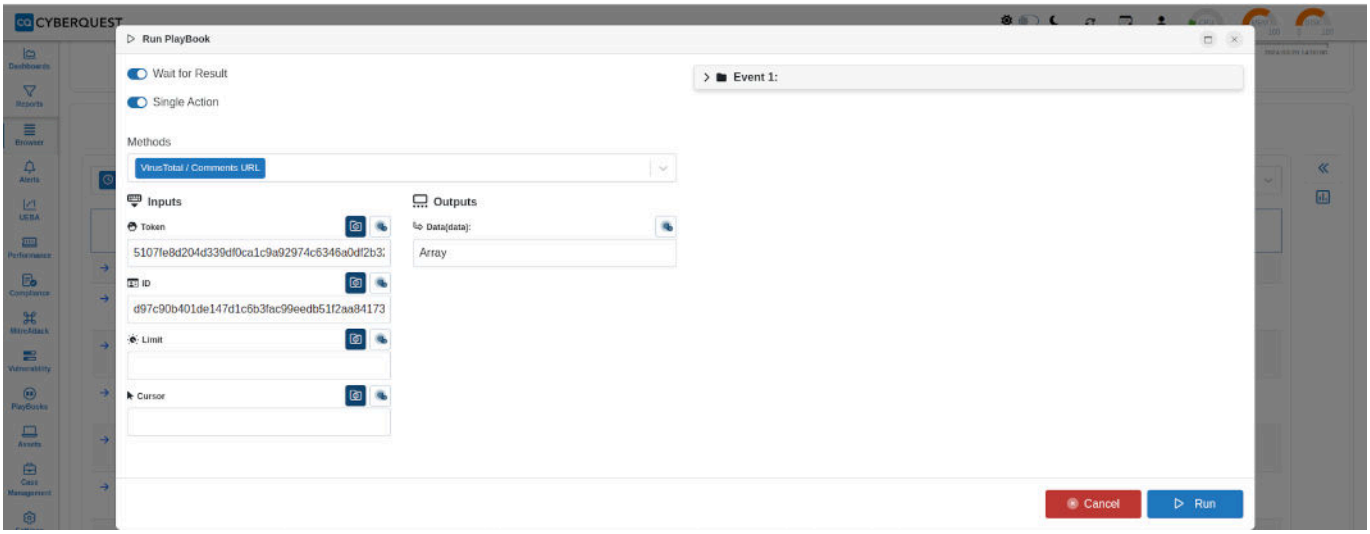


Inputs	Description
Token (is required)	To use the VirusTotal API, you must have an API key.
ID (is required)	The ID given by VirusTotal for investigation of URL
Text (is required)	The content of the comment

Outputs	Description
Data (data)	The results of the API call

VirusTotal/Comments URL method

Returns a list of Comment objects.

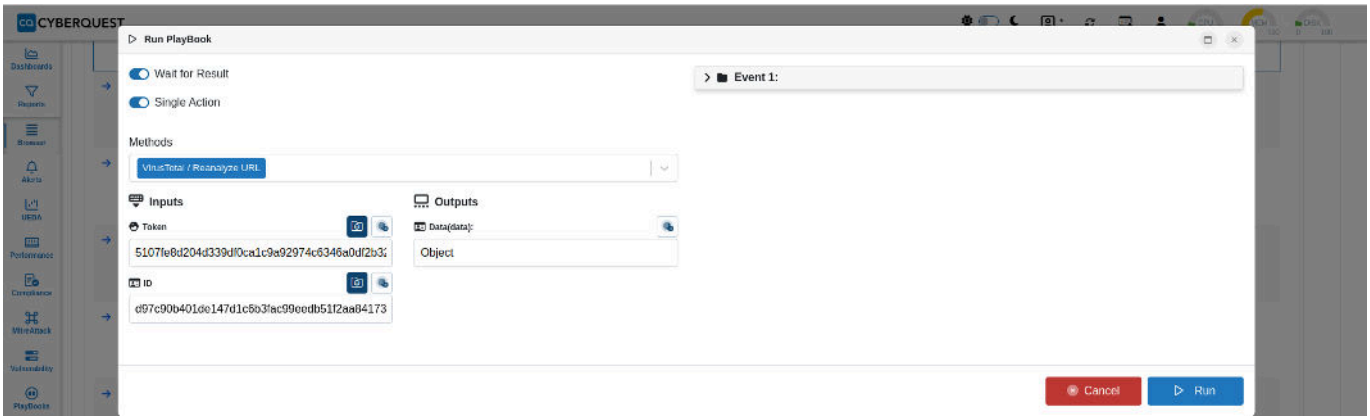


Inputs	Description
Token (is required)	To use the VirusTotal API, you must have an API key.
ID (is required)	The ID given by VirusTotal for investigation of URL
Limit	Maximum number of related objects to retrieve
Cursor	Continuation cursor

Outputs	Description
Data (data)	The comments for the investigated URL

VirusTotal/Reanalyze URL method

Request a URL rescan.

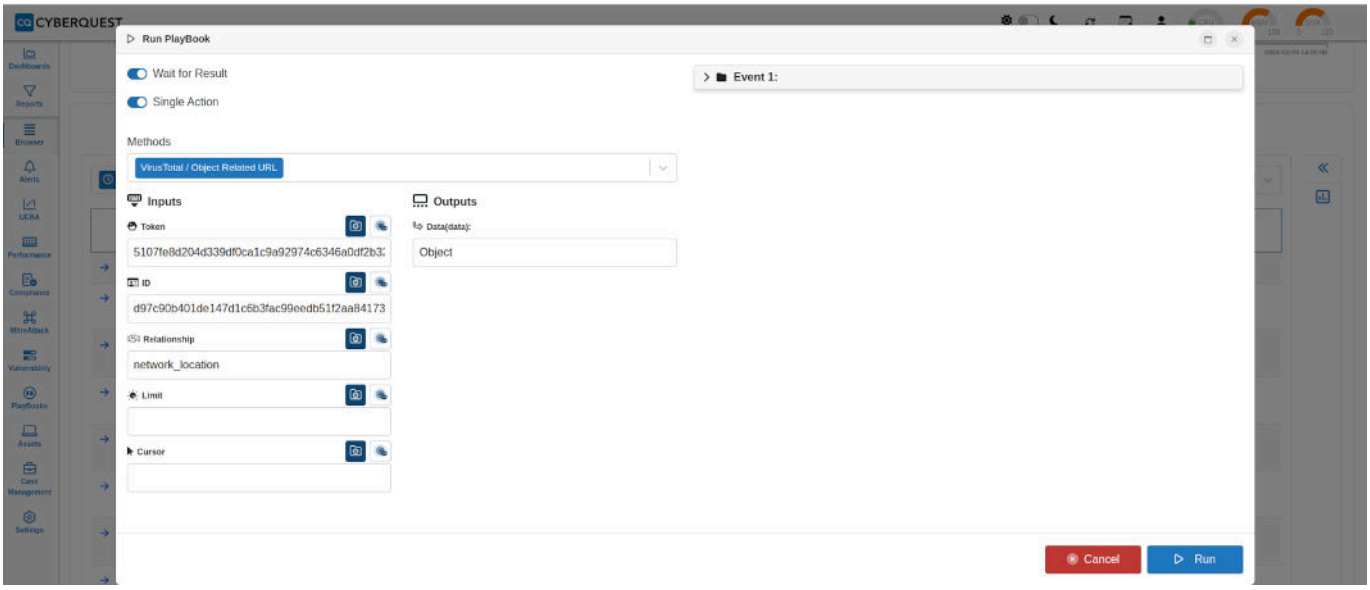


Inputs	Description
Token (is required)	To use the VirusTotal API, you must have an API key.
ID (is required)	The ID given by VirusTotal for investigation of URL

Outputs	Description
Data (data)	The results of the API call

VirusTotal/Object Related URL method

URL objects have number of relationships to other URLs and objects.

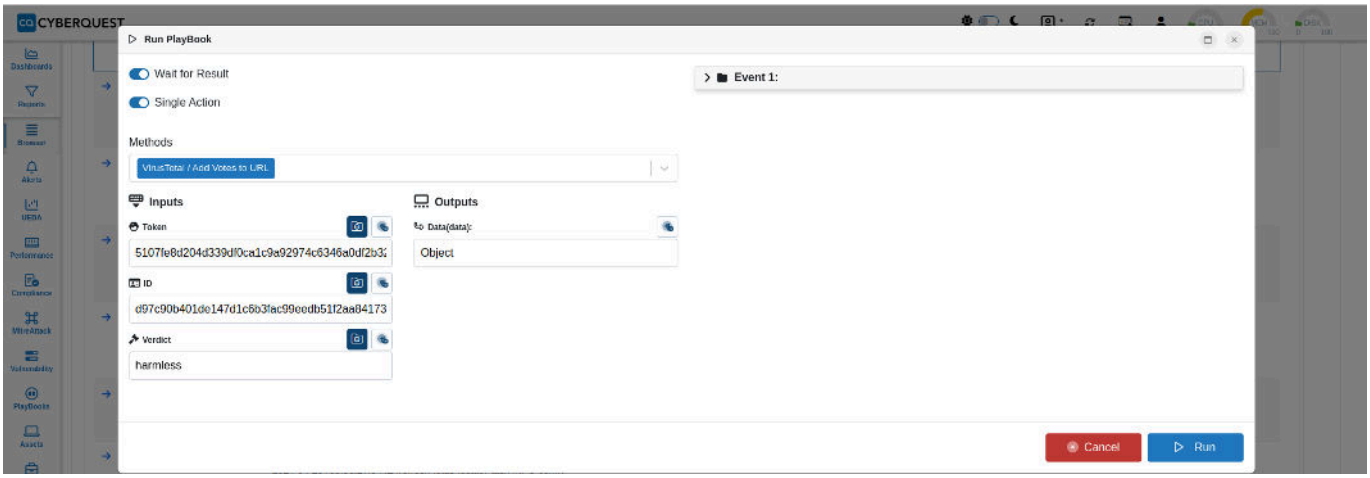


Inputs	Description
Token (is required)	To use the VirusTotal API, you must have an API key.
ID (is required)	The ID given by VirusTotal for investigation of URL
Relationship (is required)	Relationship name
Limit	Maximum number of related objects to retrieve
Cursor	Continuation cursor

Outputs	Description
Data (data)	The results of the API call

VirusTotal/Add Votes to URL method

With this endpoint you can post a vote for a given URL.

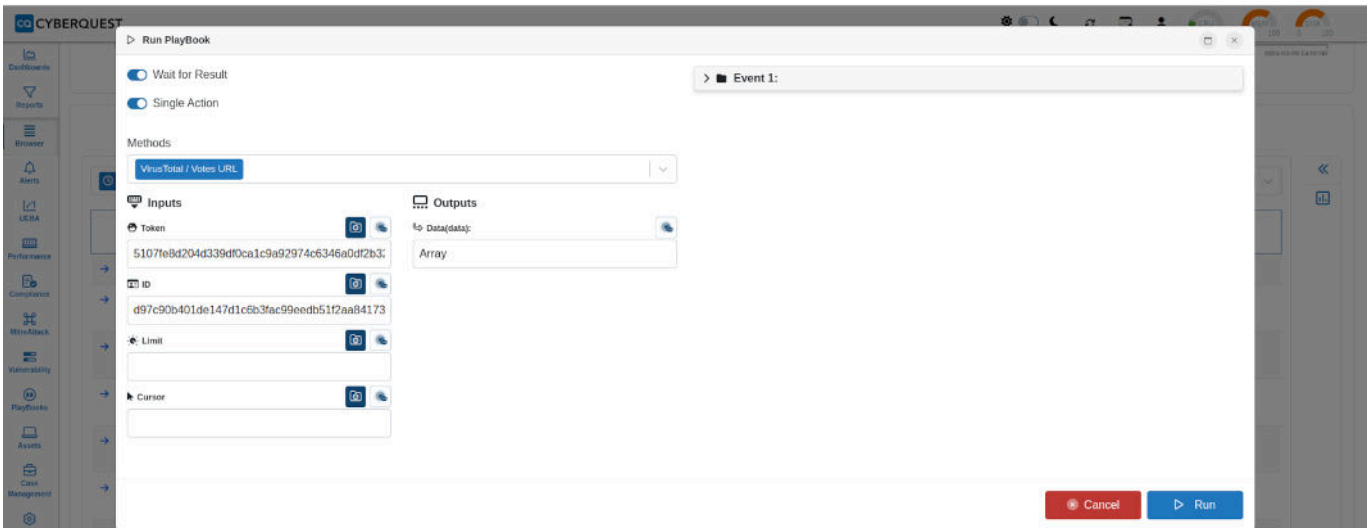


Inputs	Description
Token (is required)	To use the VirusTotal API, you must have an API key.
ID (is required)	The ID given by VirusTotal for investigation of URL
Verdict (is required)	The verdict of the vote

Outputs	Description
Data (data)	The results of the API call

VirusTotal/Votes URL method

Receive URL votes.

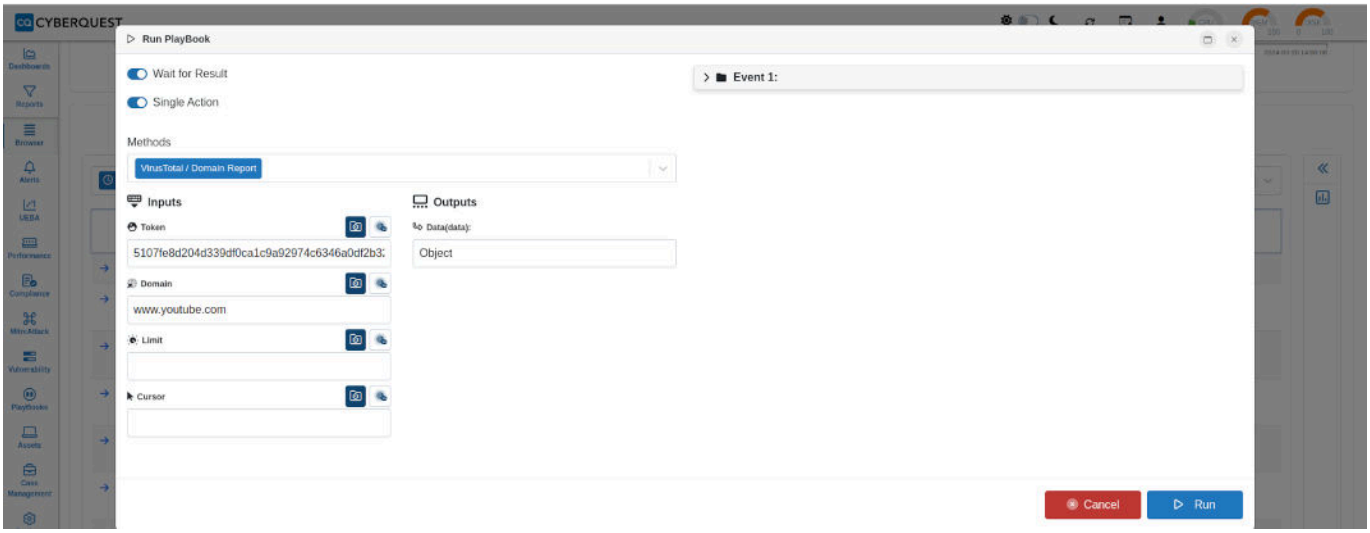


Inputs	Description
Token (is required)	To use the VirusTotal API, you must have an API key.
ID (is required)	The ID given by VirusTotal for investigation of URL
Limit	Maximum number of related objects to retrieve
Cursor	Continuation cursor

Outputs	Description
Data (data)	The votes for the investigated URL

VirusTotal/Domain Report method

Get domain report.

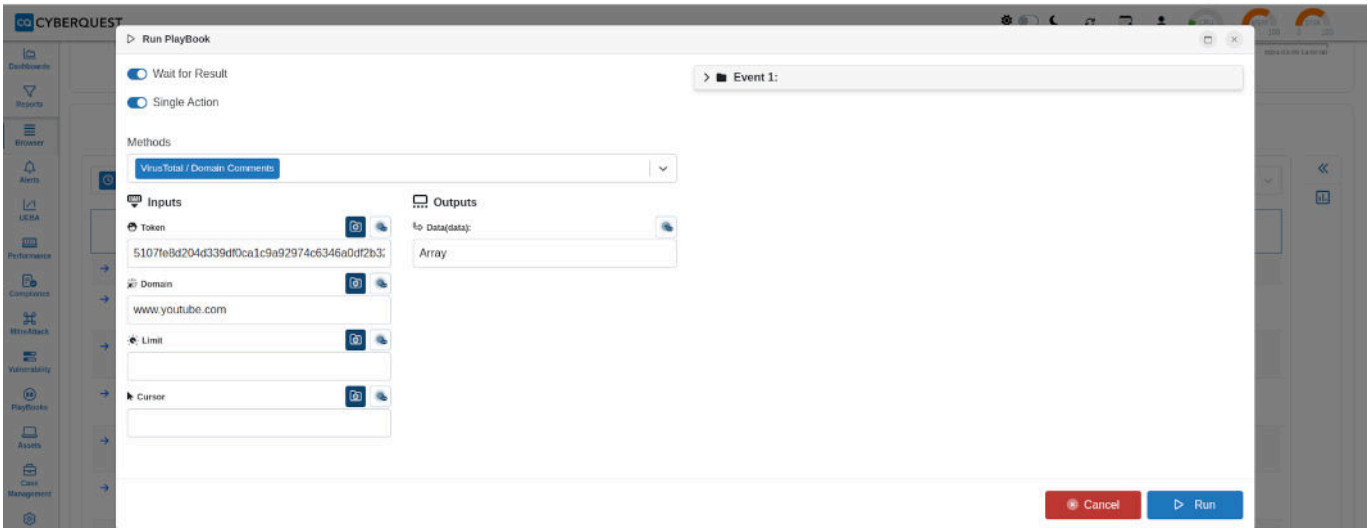


Inputs	Description
Token (is required)	To use the VirusTotal API, you must have an API key.
Domain (is required)	The domain which is investigated
Limit	Maximum number of related objects to retrieve
Cursor	Continuation cursor

Outputs	Description
Data (data)	The results of the API call

VirusTotal/Domain Comments method

Get comments on a domain.

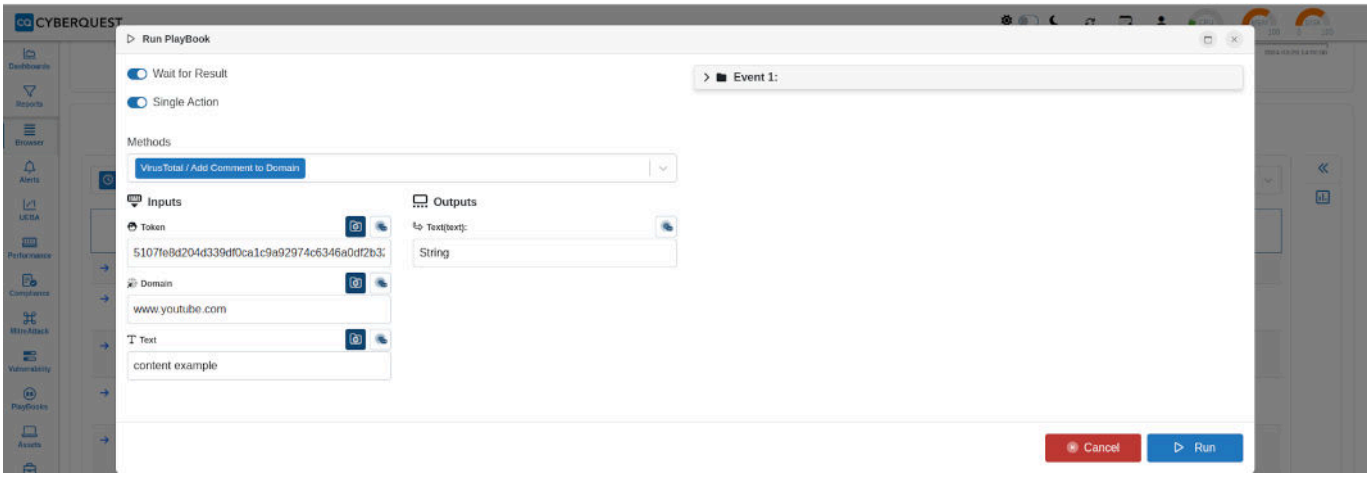


Inputs	Description
Token (is required)	To use the VirusTotal API, you must have an API key.
Domain (is required)	The domain which is investigated
Limit	Maximum number of related objects to retrieve
Cursor	Continuation cursor

Outputs	Description
Data (data)	The List of comments for the domain which is investigated

VirusTotal/Add Comment to Domain method

Add a comment to a domain.

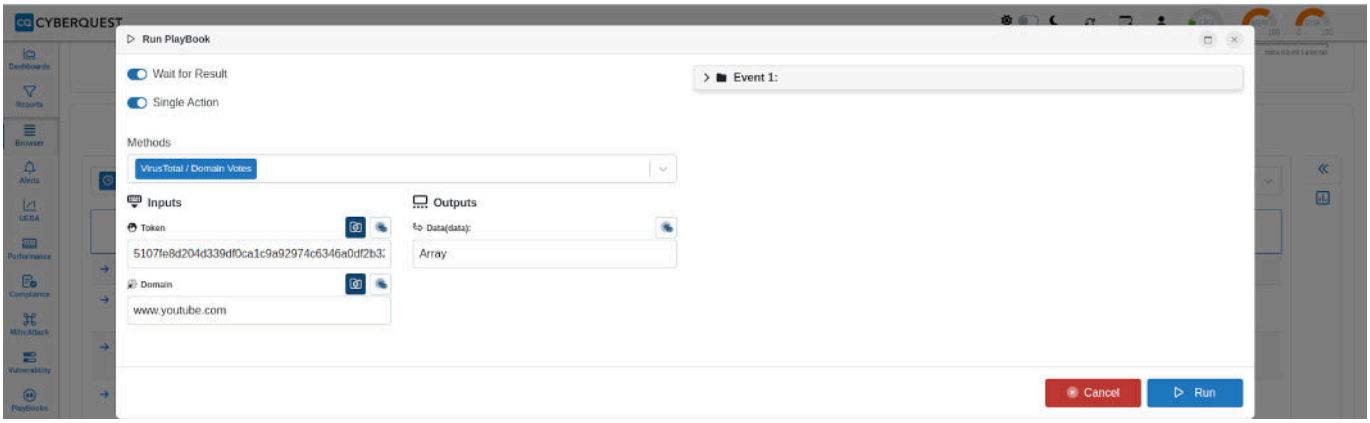


Inputs	Description
Token (is required)	To use the VirusTotal API, you must have an API key.
Domain (is required)	The domain which is investigated
Text (is required)	The content of the comment

Outputs	Description
Text (text)	The content of the comment

VirusTotal/Domain Votes method

Get votes on a domain.

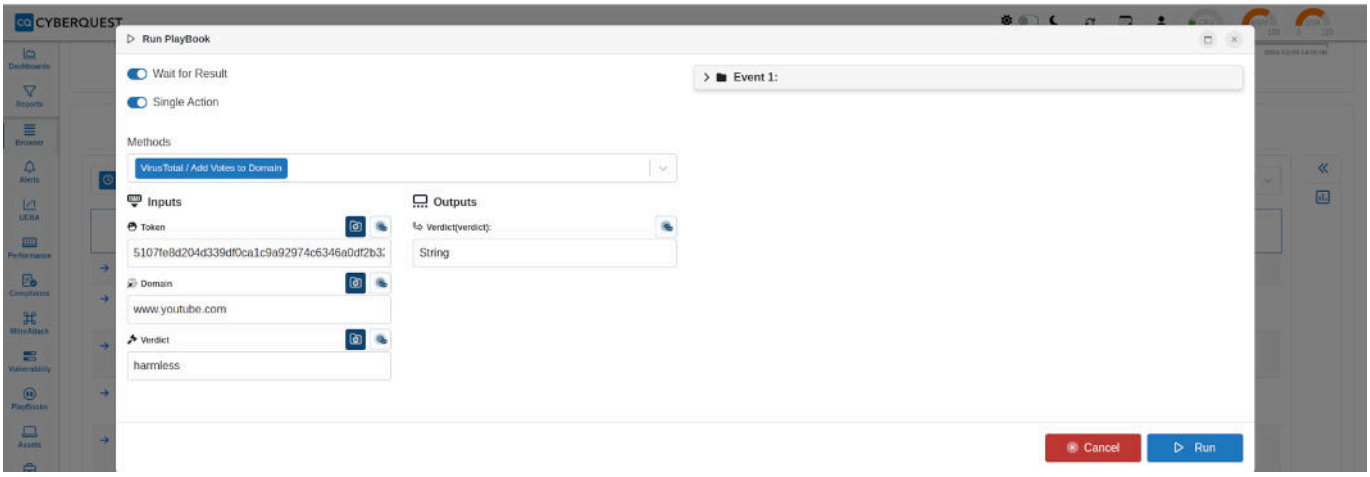


Inputs	Description
Token (is required)	To use the VirusTotal API, you must have an API key.
Domain (is required)	The domain which is investigated

Outputs	Description
Data (data)	A list with votes of the investigated domain

VirusTotal/Add Votes to Domain method

Add a vote to a domain.

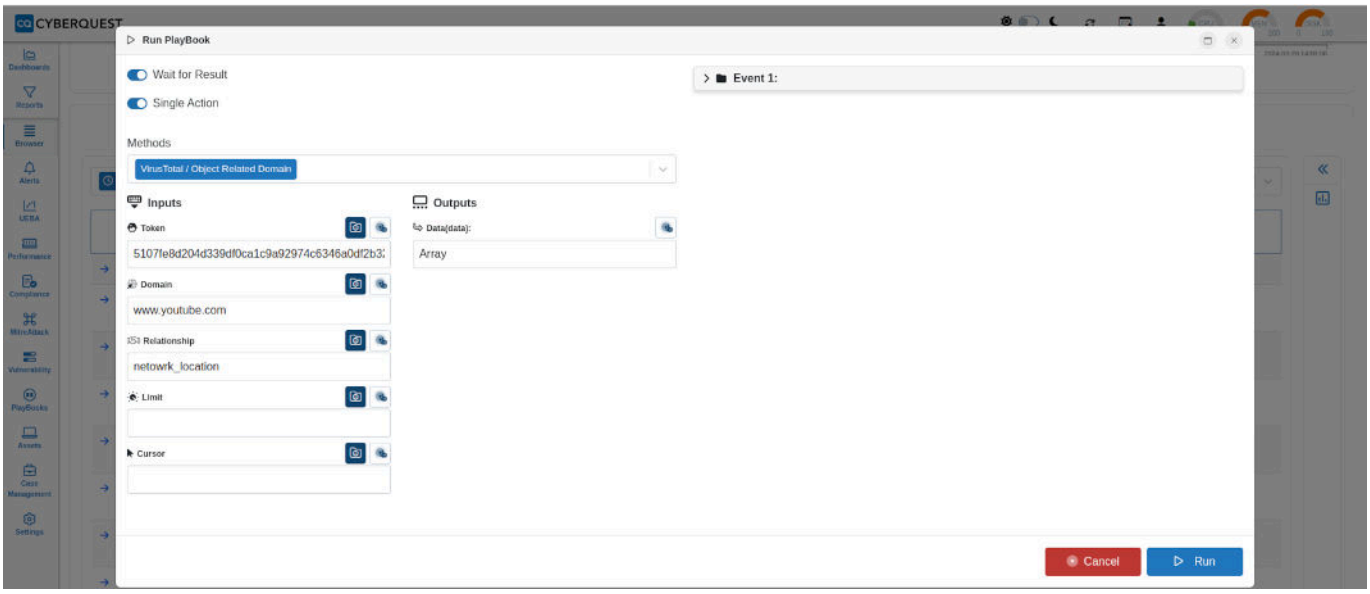


Inputs	Description
Token (is required)	To use the VirusTotal API, you must have an API key.
Domain (is required)	The domain which is investigated
Verdict (is required)	The type of verdict

Outputs	Description
Verdict (verdict)	The result of the vote (malicious or harmless)

VirusTotal/Object Related Domain method

Receive objects related to a domain.

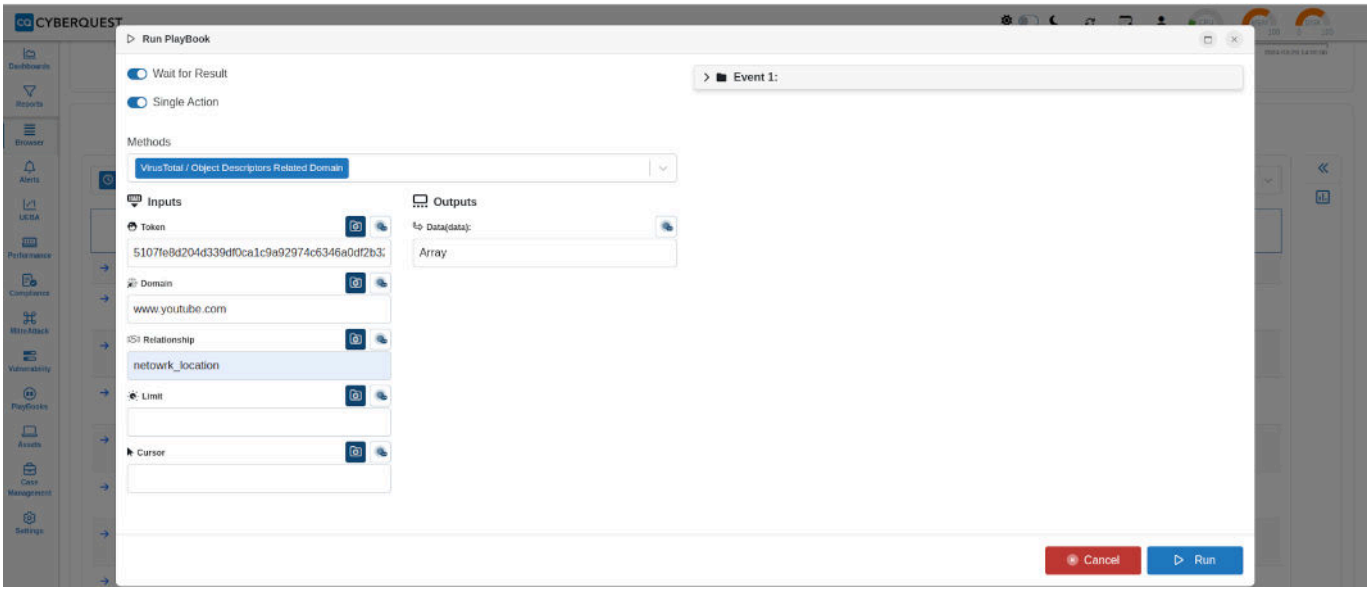


Inputs	Description
Token (is required)	To use the VirusTotal API, you must have an API key.
Domain (is required)	The domain which is investigated
Relationship (is required)	Relationship name
Limit	Maximum number of related objects to retrieve
Cursor	Continuation cursor

Outputs	Description
Data (data)	The Object Related Domain

VirusTotal/Object Descriptors Related Domain method

Receive object descriptors related to a domain.

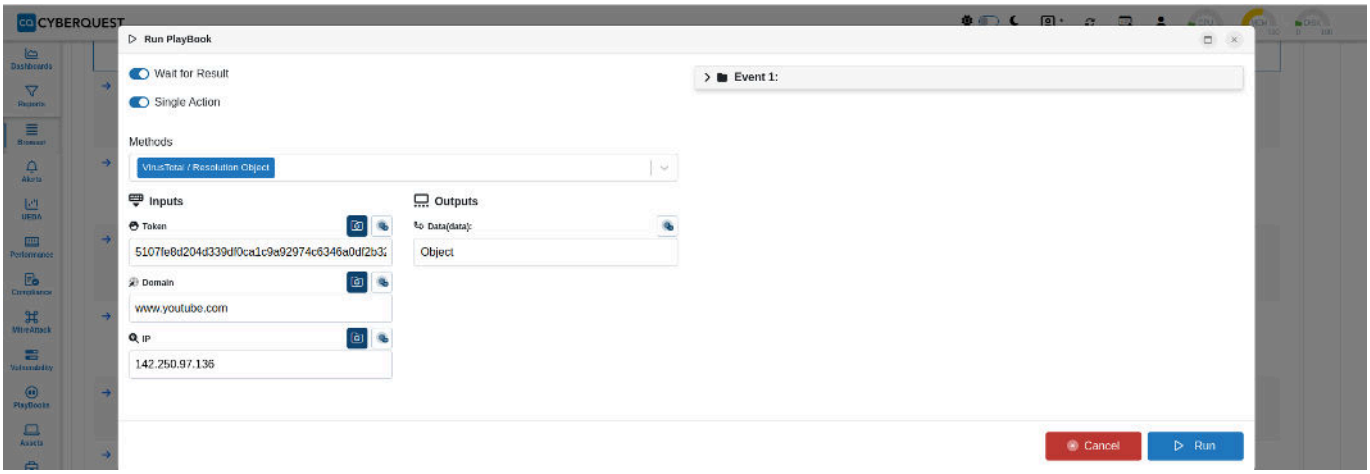


Inputs	Description
Token (is required)	To use the VirusTotal API, you must have an API key.
Domain (is required)	The domain which is investigated
Relationship (is required)	Relationship name
Limit	Maximum number of related objects to retrieve
Cursor	Continuation cursor

Outputs	Description
Data (data)	The Object Descriptors Related to Domain

VirusTotal/Resolution Object method

Receive a DNS resolution object.

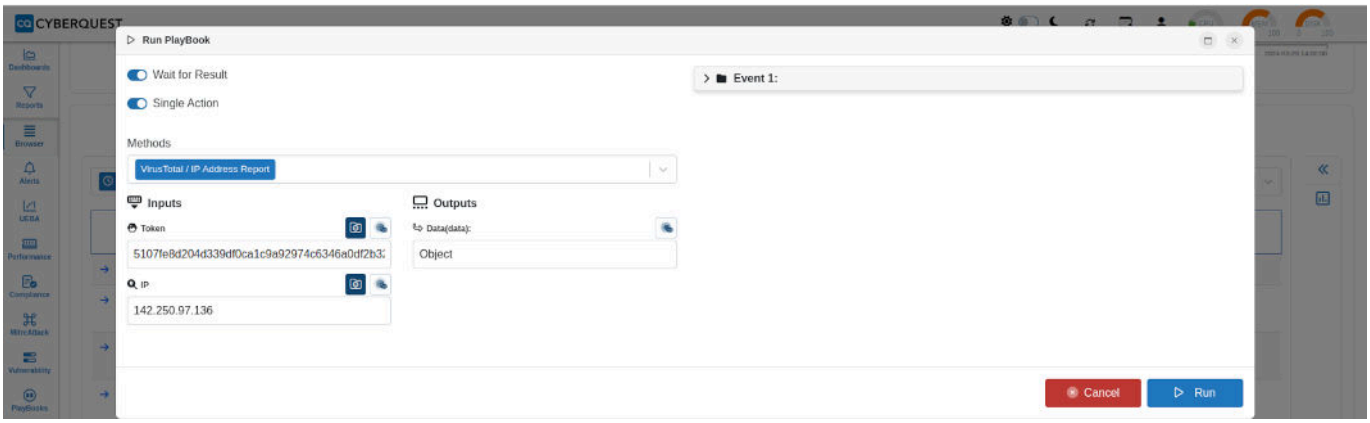


Inputs	Description
Token (is required)	To use the VirusTotal API, you must have an API key.
Domain (is required)	The domain which is investigated
IP (is required)	The IP of the domain which is investigated

Outputs	Description
Data (data)	The results of the API call

VirusTotal/IP Address Report method

Get an IP address report.

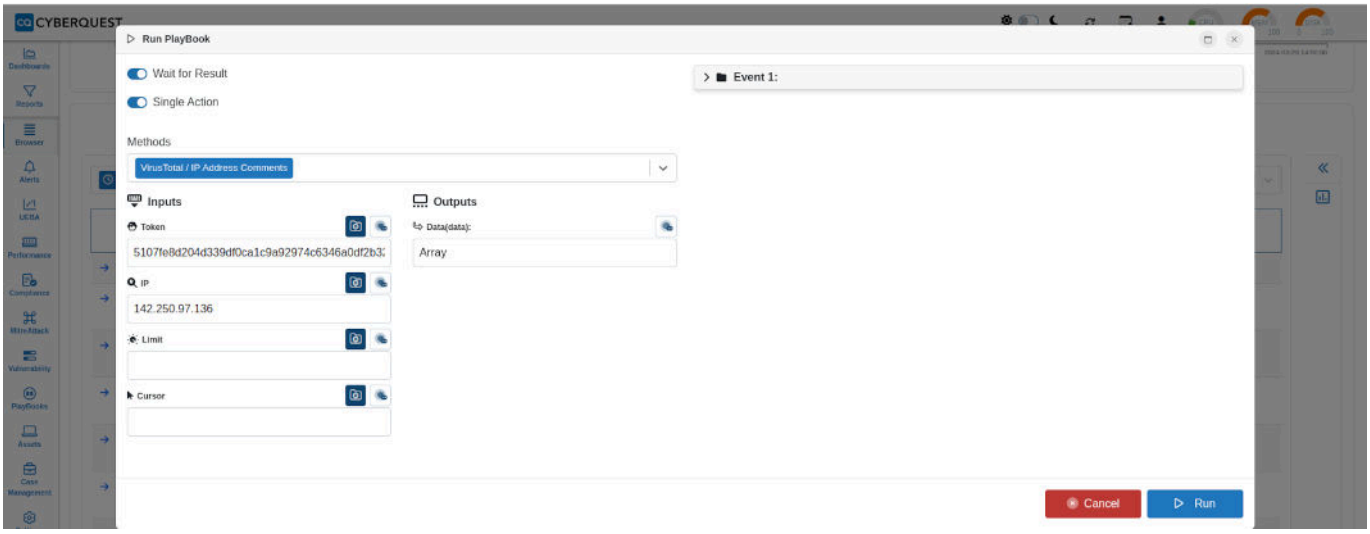


Inputs	Description
Token (is required)	To use the VirusTotal API, you must have an API key.
IP (is required)	The IP which is investigated

Outputs	Description
Data (data)	It provides a concise summary of cryptographic parameters used in the TLS handshake, helping to identify and classify network traffic

VirusTotal/IP Address Comments method

Get comments on an IP address.

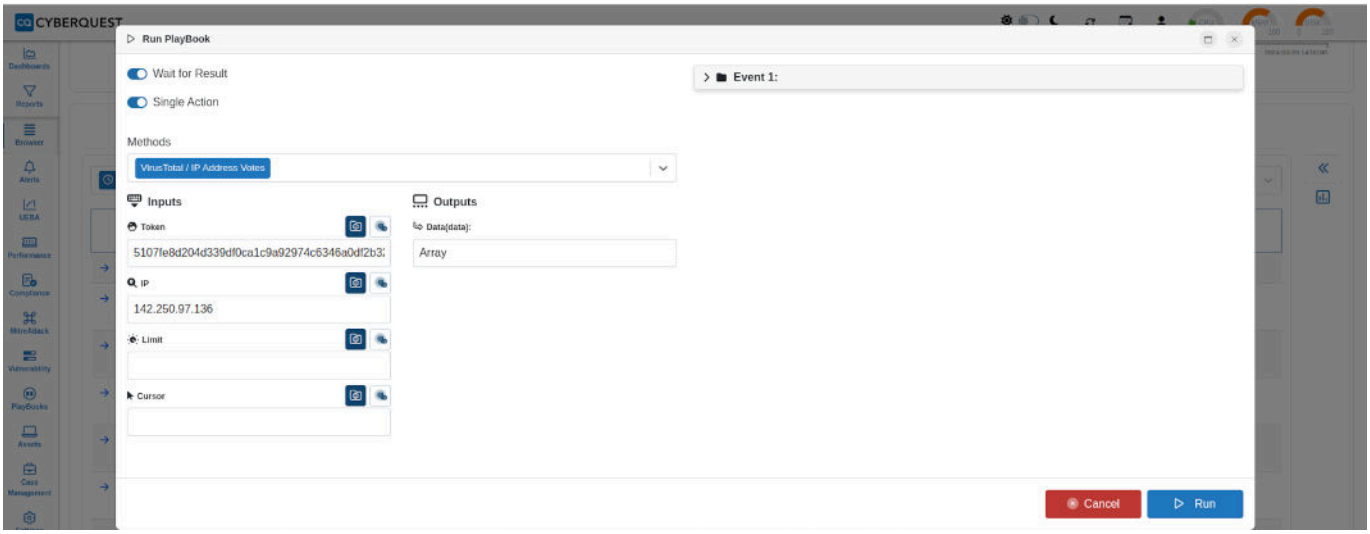


Inputs	Description
Token (is required)	To use the VirusTotal API, you must have an API key.
IP (is required)	The IP which is investigated
Limit	Maximum number of related objects to retrieve
Cursor	Continuation cursor

Outputs	Description
Data (data)	The comments for the investigated IP

VirusTotal/IP Address Votes method

Get votes on an IP address.

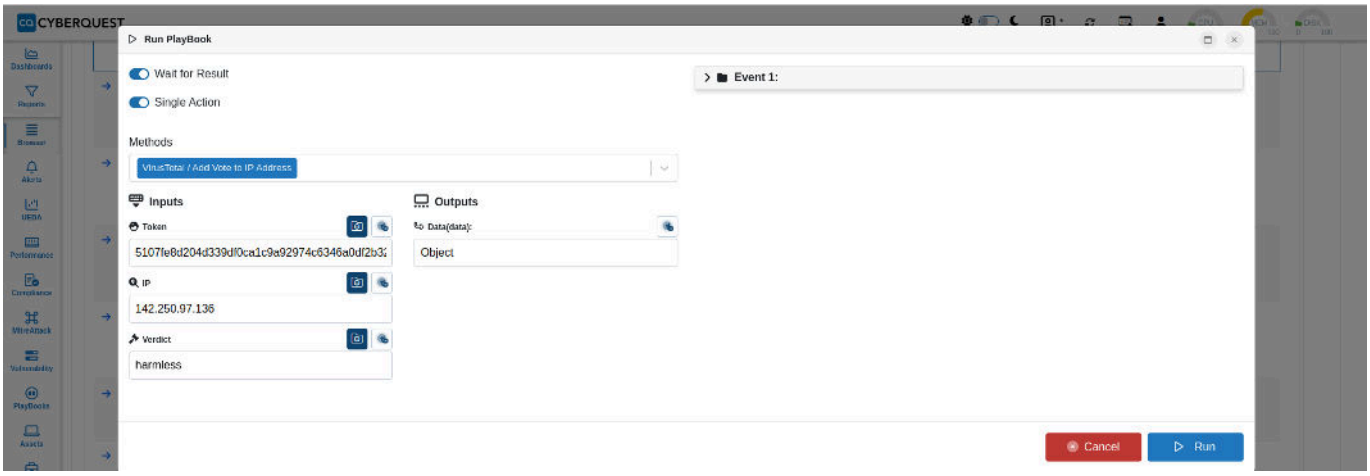


Inputs	Description
Token (is required)	To use the VirusTotal API, you must have an API key.
IP (is required)	The IP which is investigated
Limit	Maximum number of related objects to retrieve
Cursor	Continuation cursor

Outputs	Description
Data (data)	The results of the API call

VirusTotal/Add Vote to IP Address method

With this endpoint you can post a vote for a given IP address.

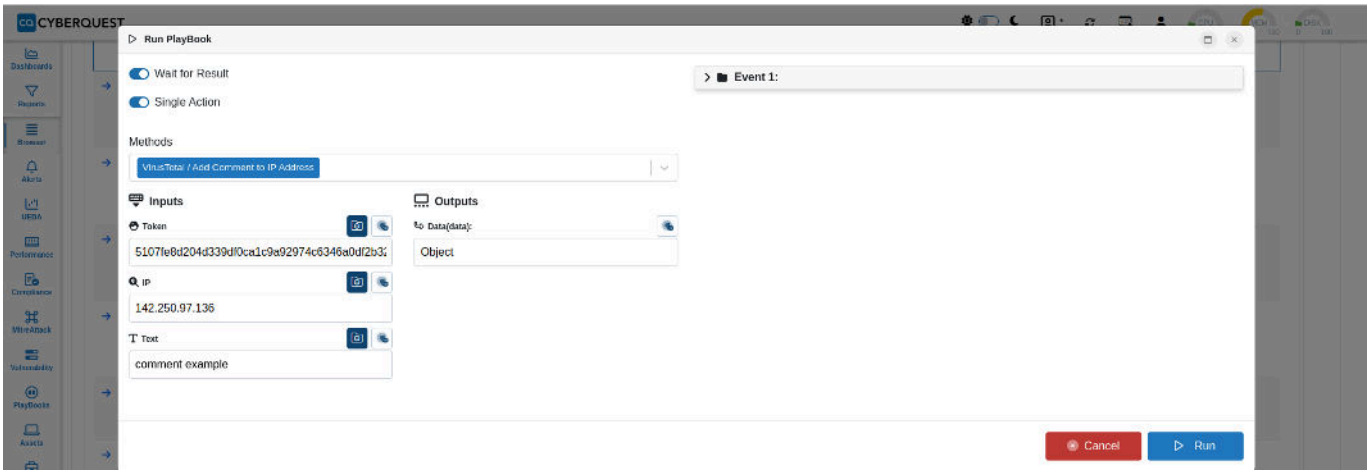


Inputs	Description
Token (is required)	To use the VirusTotal API, you must have an API key.
IP (is required)	The IP which is investigated
Verdict (is required)	The verdict of the vote

Outputs	Description
Data (data)	The result of the vote (malicious or harmless)

VirusTotal/Add Comment to IP Address method

With this endpoint you can post a comment for a given IP address.

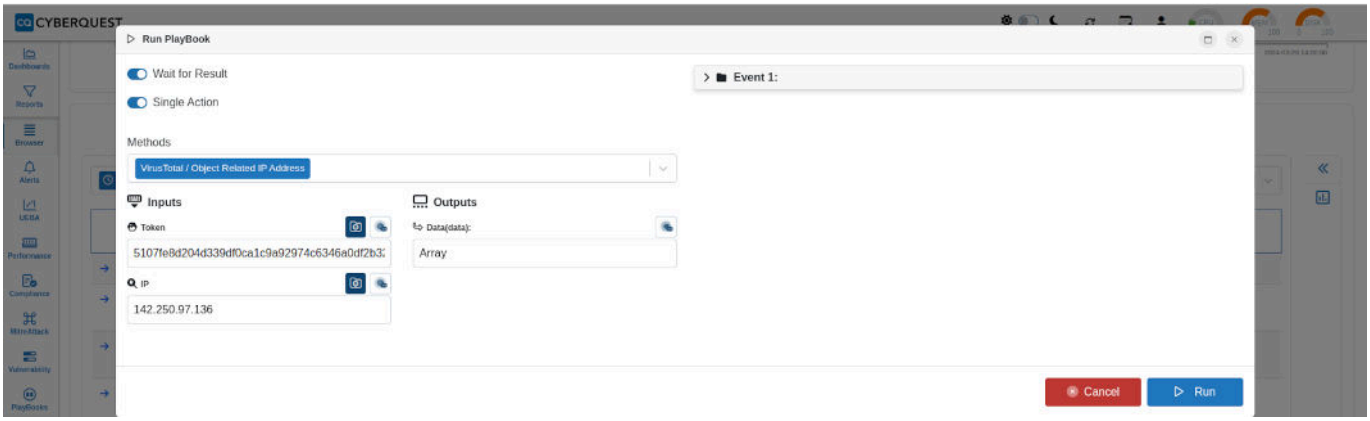


Inputs	Description
Token (is required)	To use the VirusTotal API, you must have an API key.
IP (is required)	The IP which is investigated
Text (is required)	The content of the comment

Outputs	Description
Data (data)	The results of the API call

VirusTotal/Object Related IP Address method

Get objects related to an IP address.

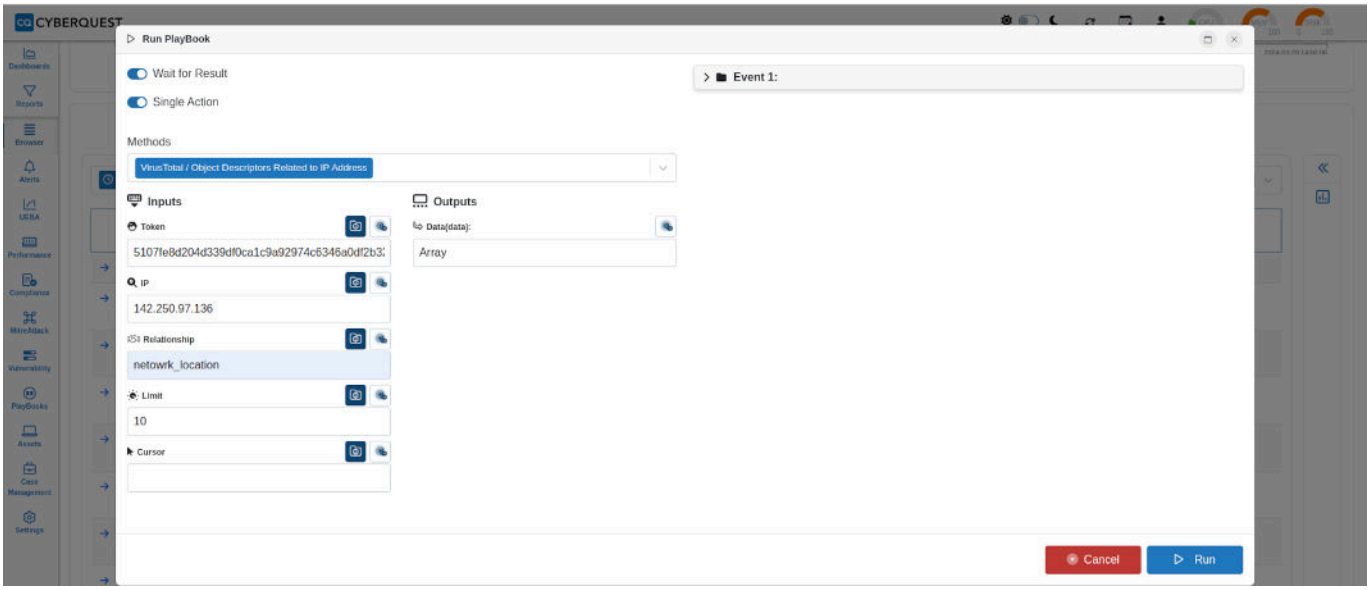


Inputs	Description
Token (is required)	To use the VirusTotal API, you must have an API key.
IP (is required)	The IP which is investigated

Outputs	Description
Data (data)	The objects related to IP address investigated

VirusTotal/Object Descriptors Related to IP Address method

Get object descriptors related to an IP address.

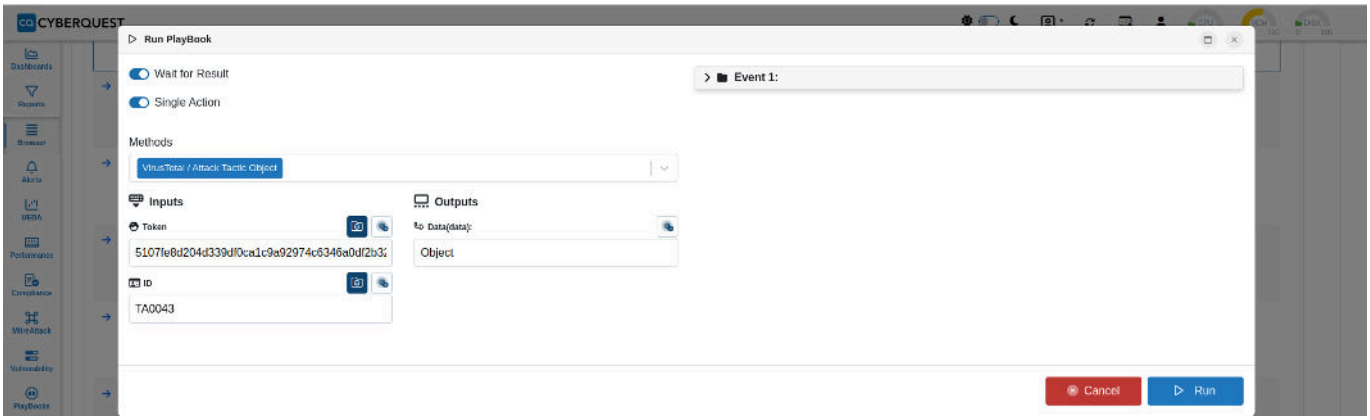


Inputs	Description
Token (is required)	To use the VirusTotal API, you must have an API key.
IP (is required)	The IP which is investigated
Relationship (is required)	Relationship name
Limit	Maximum number of related objects to retrieve
Cursor	Continuation cursor

Outputs	Description
Data (data)	The object descriptors for the IP which is investigated

VirusTotal/Attack Tactic Object method

Get objects related to an attack tactic.

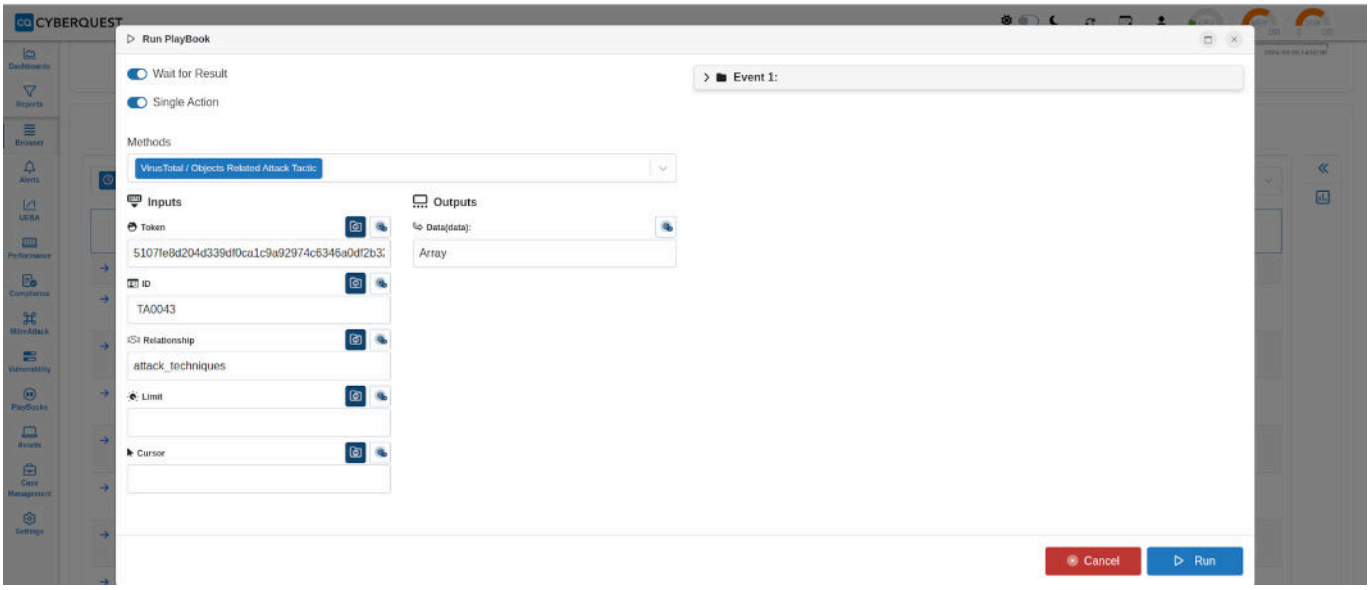


Inputs	Description
Token (is required)	To use the VirusTotal API, you must have an API key.
ID (is required)	Attack tactics ID

Outputs	Description
Data (data)	The results of the API call

VirusTotal/Objects Related Attack Tactic method

Get objects related to an attack tactic.

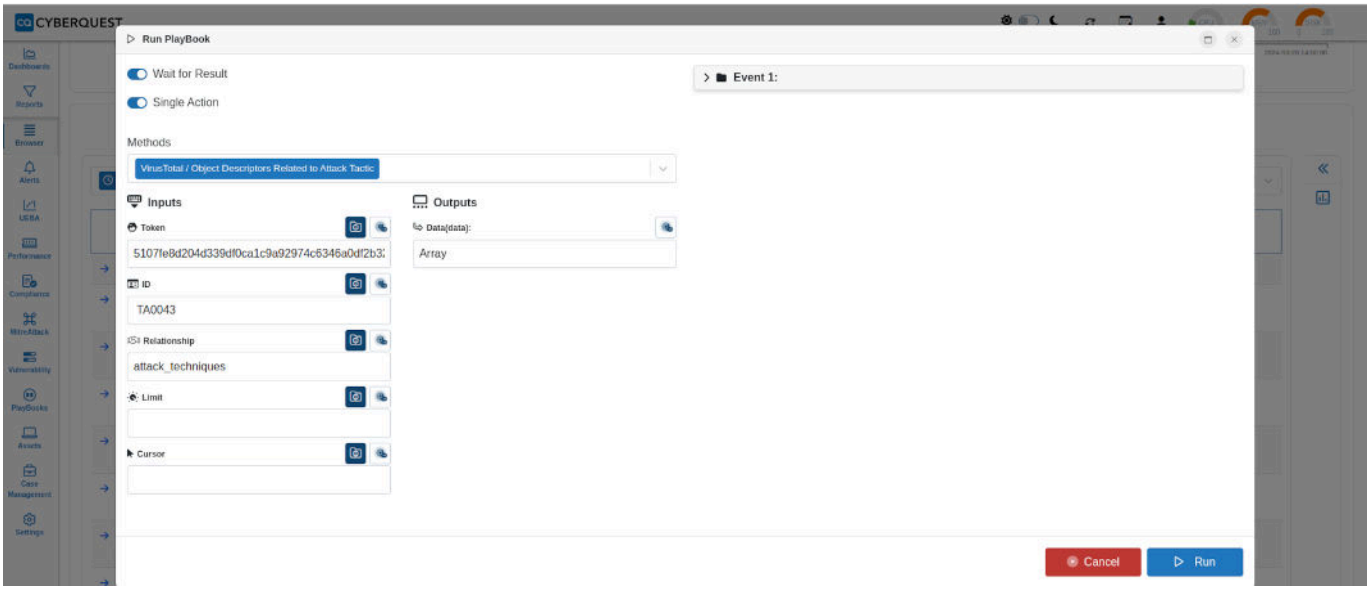


Inputs	Description
Token (is required)	To use the VirusTotal API, you must have an API key.
ID (is required)	Attack tactics ID
Relationship (is required)	Relationship name
Limit	Maximum number of related objects to retrieve
Cursor	Continuation cursor

Outputs	Description
Data (data)	Results for the Object Related Tactic Requested

VirusTotal/Object Descriptors Related to Attack Tactic method

Get object descriptors related to an attack tactic.

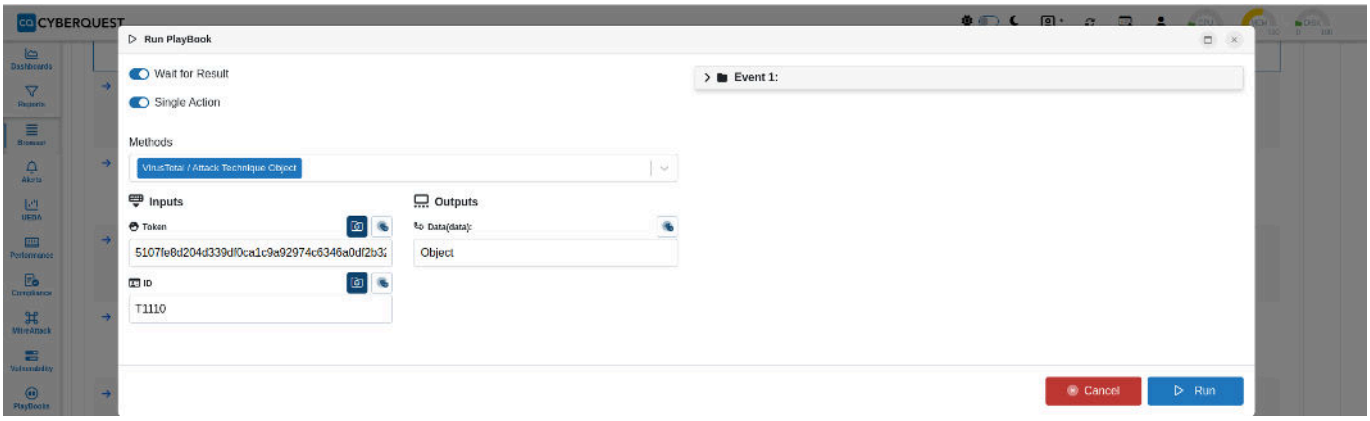


Inputs	Description
Token (is required)	To use the VirusTotal API, you must have an API key.
ID (is required)	Attack tactics ID
Relationship (is required)	Relationship name
Limit	Maximum number of related objects to retrieve
Cursor	Continuation cursor

Outputs	Description
Data (data)	Results for the Object Descriptors Related Tactic Requested

VirusTotal/Attack Technique Object method

Get an attack technique object.

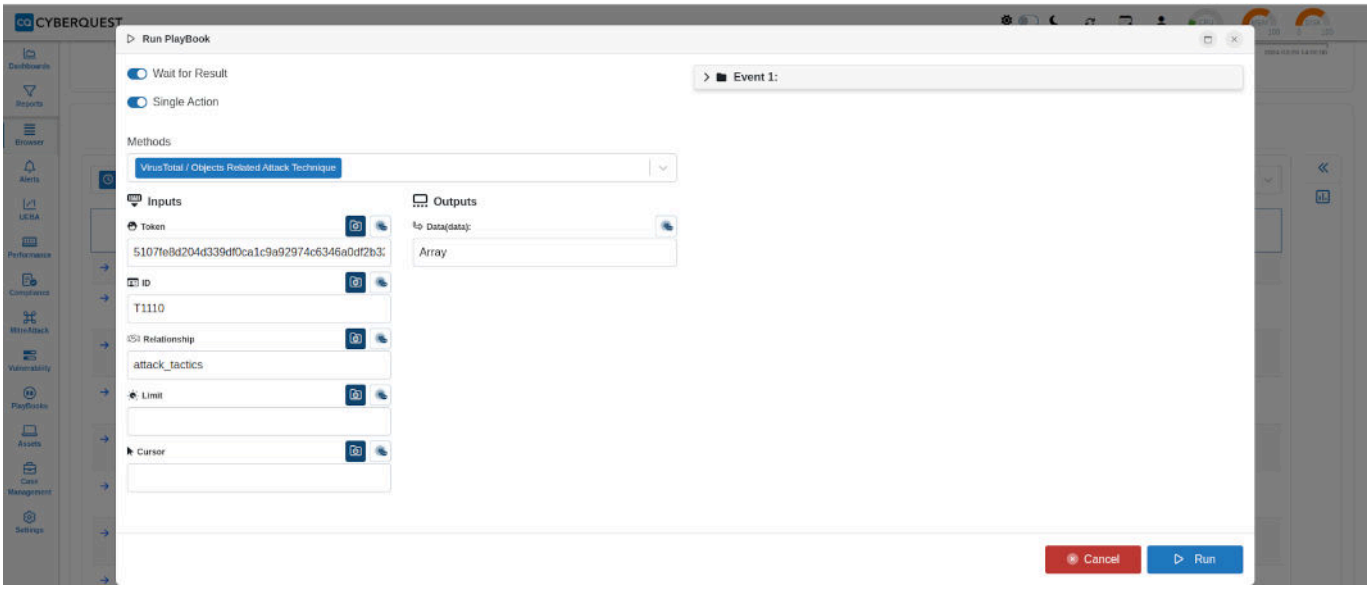


Inputs	Description
Token (is required)	To use the VirusTotal API, you must have an API key.
ID (is required)	Attack techniques ID

Outputs	Description
Data (data)	The results of the API call

VirusTotal/Objects Related Attack Technique method

Get objects related to an attack technique.

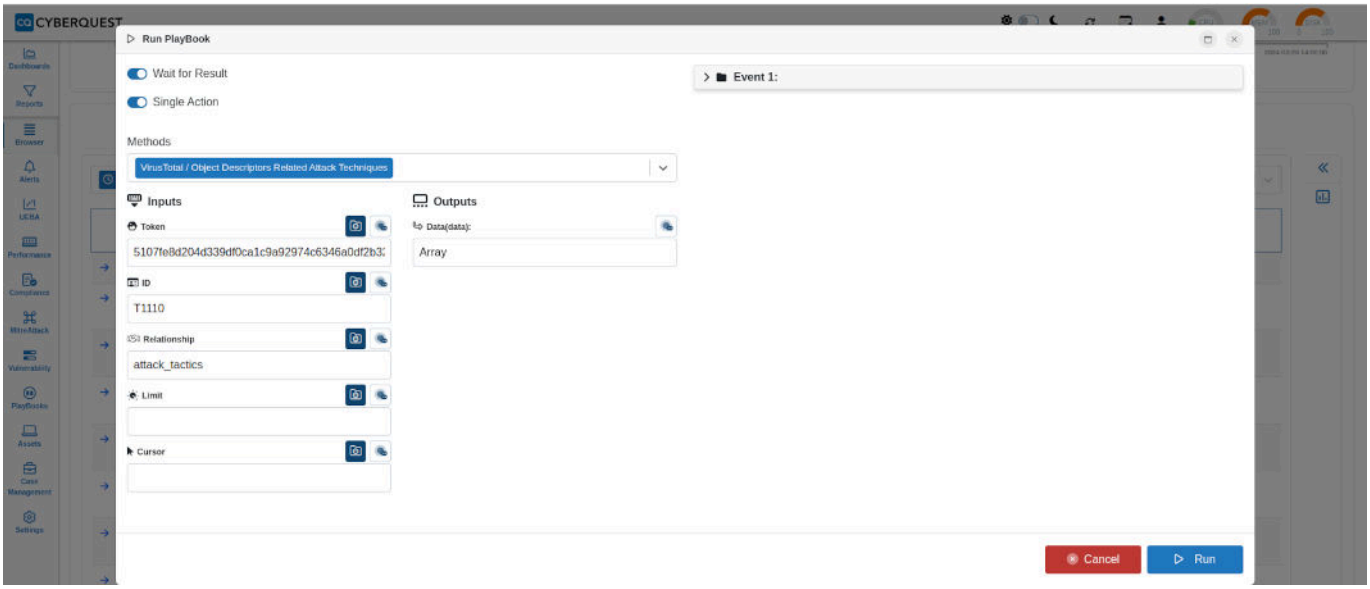


Inputs	Description
Token (is required)	To use the VirusTotal API, you must have an API key.
ID (is required)	Attack techniques ID
Relationship (is required)	Relationship name
Limit	Maximum number of related objects to retrieve
Cursor	Continuation cursor

Outputs	Description
Data (data)	The results of the API call

VirusTotal/Object Descriptors Related Attack Techniques method

Get object descriptors related to an attack technique.

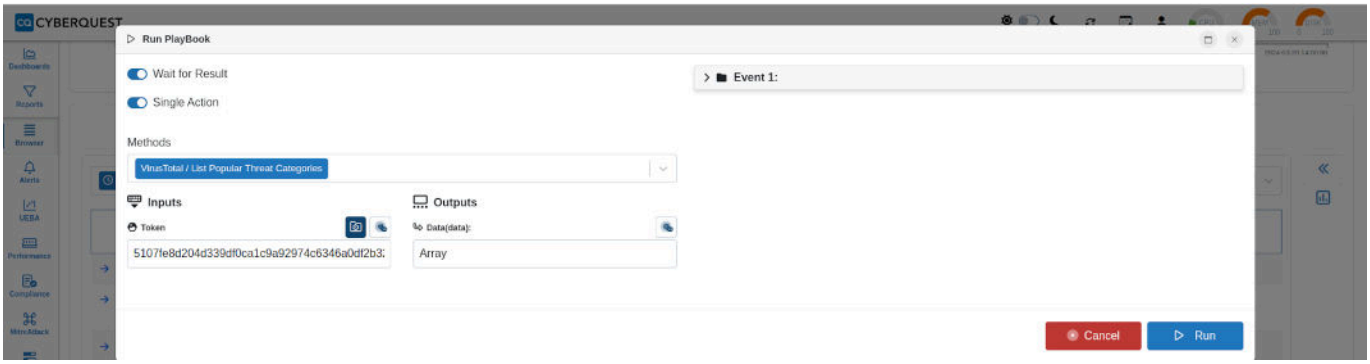


Inputs	Description
Token (is required)	To use the VirusTotal API, you must have an API key.
ID (is required)	Attack techniques ID
Relationship (is required)	Relationship name
Limit	Maximum number of related objects to retrieve
Cursor	Continuation cursor

Outputs	Description
Data (data)	The results of the API call

VirusTotal/List Popular Threat Categories method

With this endpoint you can post a comment for a given IP address.

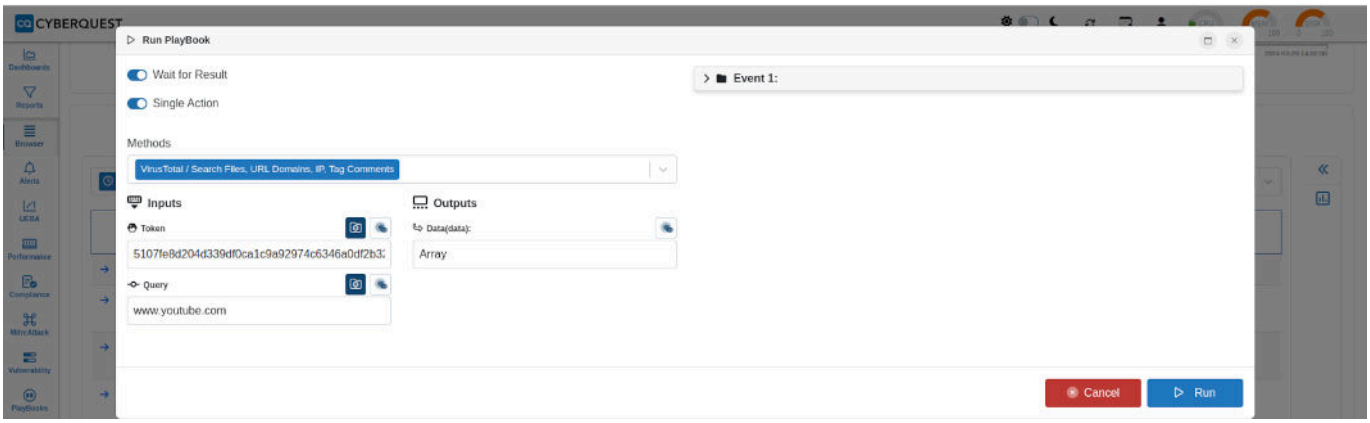


Inputs	Description
Token (is required)	To use the VirusTotal API, you must have an API key.

Outputs	Description
Data (data)	The Threat Categories of VirtusTotal

VirusTotal/Search Files, URL Domains, IP, Tag Comments method

Search files, URLs, domains, IPs and tag comments.

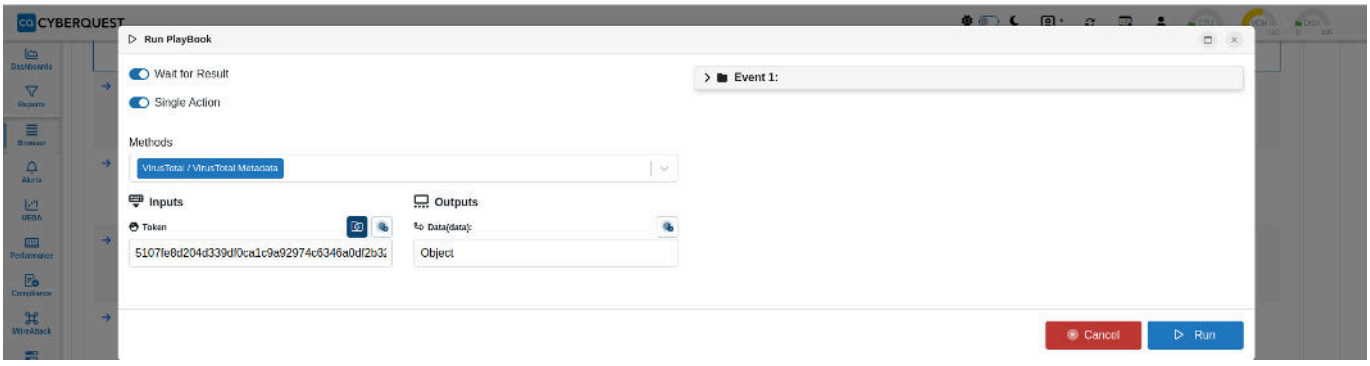


Inputs	Description
Token (is required)	To use the VirusTotal API, you must have an API key.
Query (is required)	The elements which is searched

Outputs	Description
Data (data)	The results of the search

VirusTotal/VirusTotal Metadata method

Get VirusTotal metadata.

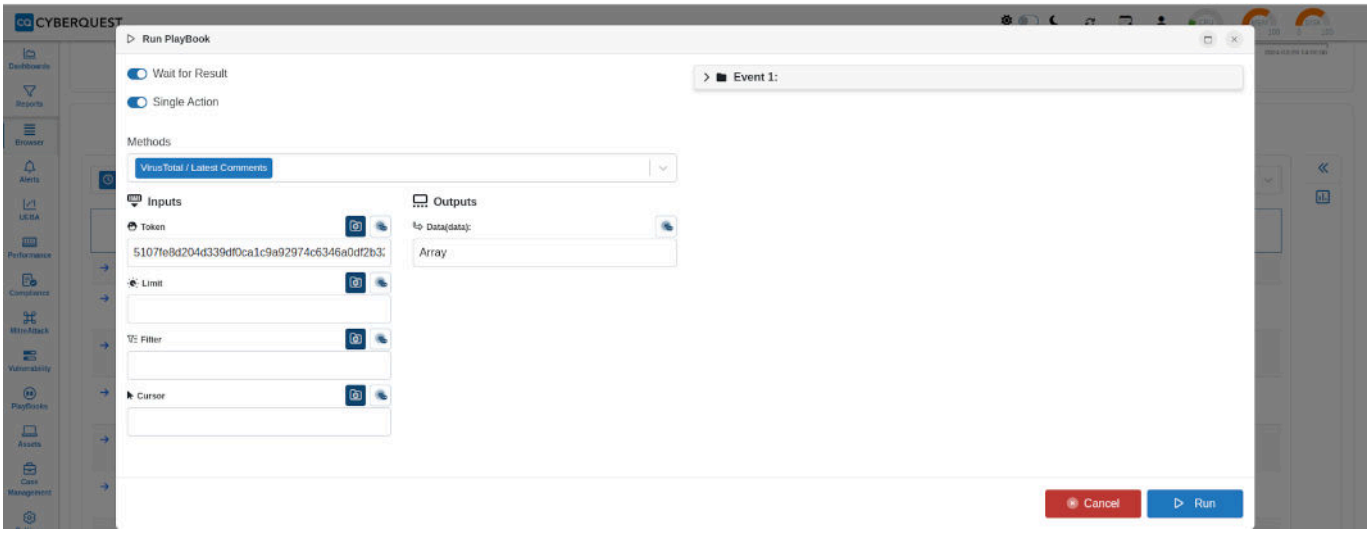


Inputs	Description
Token (is required)	To use the VirusTotal API, you must have an API key.

Outputs	Description
Data (data)	The results of the API call

VirusTotal/Latest Comments method

Get latest comments.

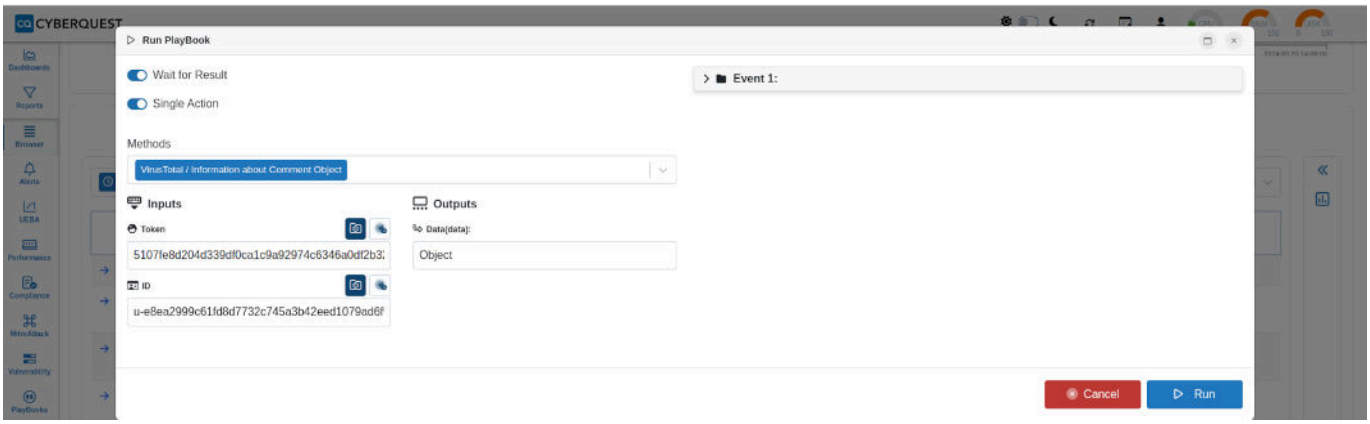


Inputs	Description
Token (is required)	To use the VirusTotal API, you must have an API key.
Limit	Maximum number of related objects to retrieve
Filter	Filter returned elements
Cursor	Continuation cursor

Outputs	Description
Data (data)	A list with latest comments

VirusTotal/Information about Comment Object method

Get a comment object.

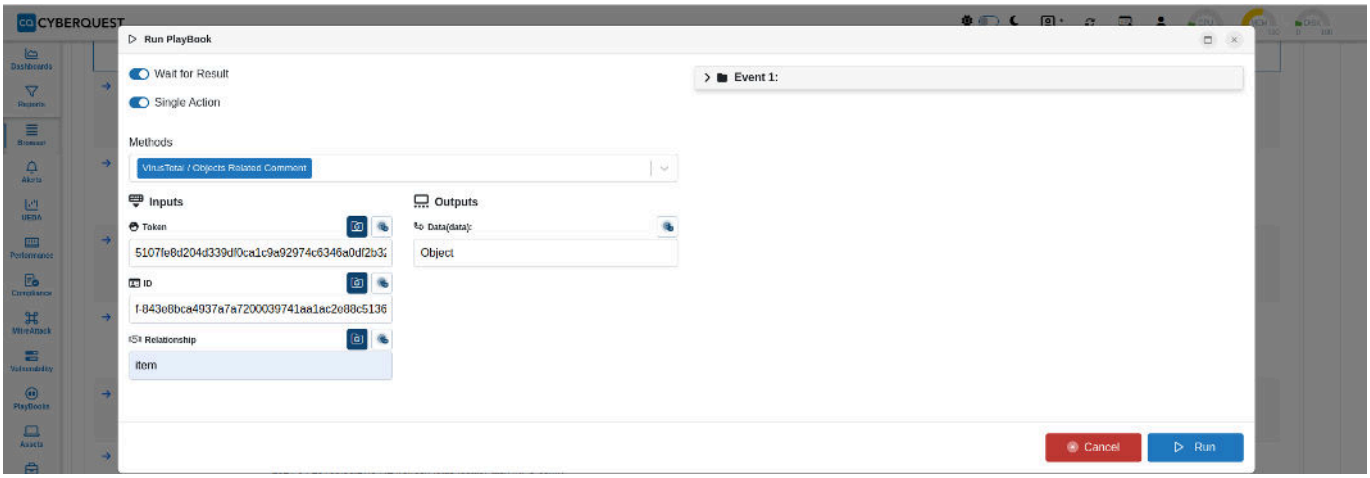


Inputs	Description
Token (is required)	To use the VirusTotal API, you must have an API key.
ID (is required)	The ID of URL or File which you want to get comments

Outputs	Description
Data (data)	The results of the API call

VirusTotal/Objects Related Comment method

Get objects related to a comment.

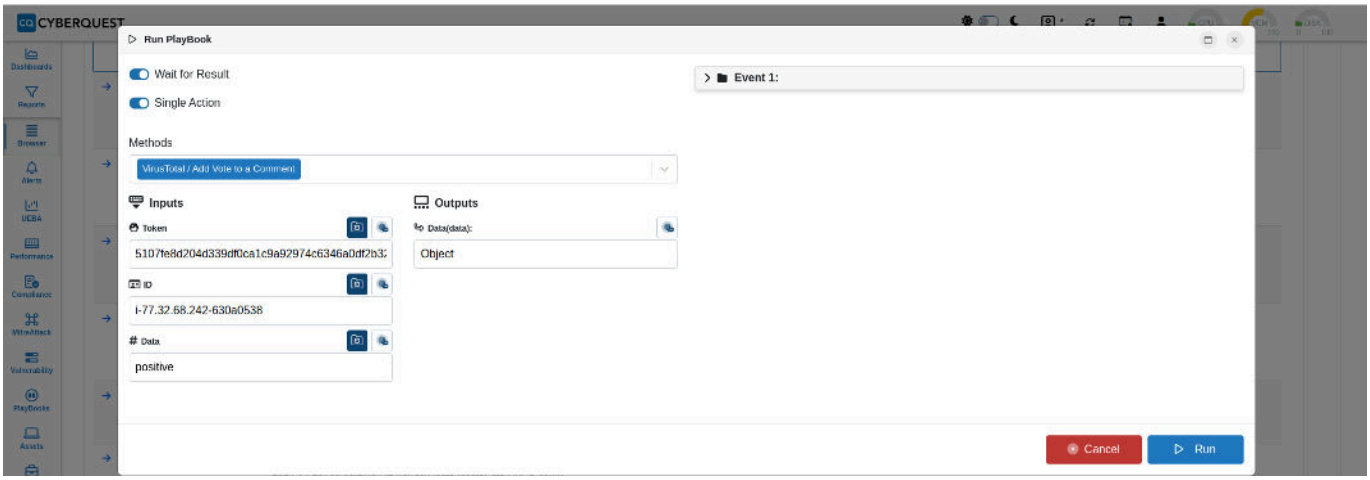


Inputs	Description
Token (is required)	To use the VirusTotal API, you must have an API key.
ID (is required)	The ID of URL or File which you want to get comments
Relationship (is required)	Relationship name

Outputs	Description
Data (data)	The results of the API call

VirusTotal/Add Vote to a Comment method

Add a vote to a comment.

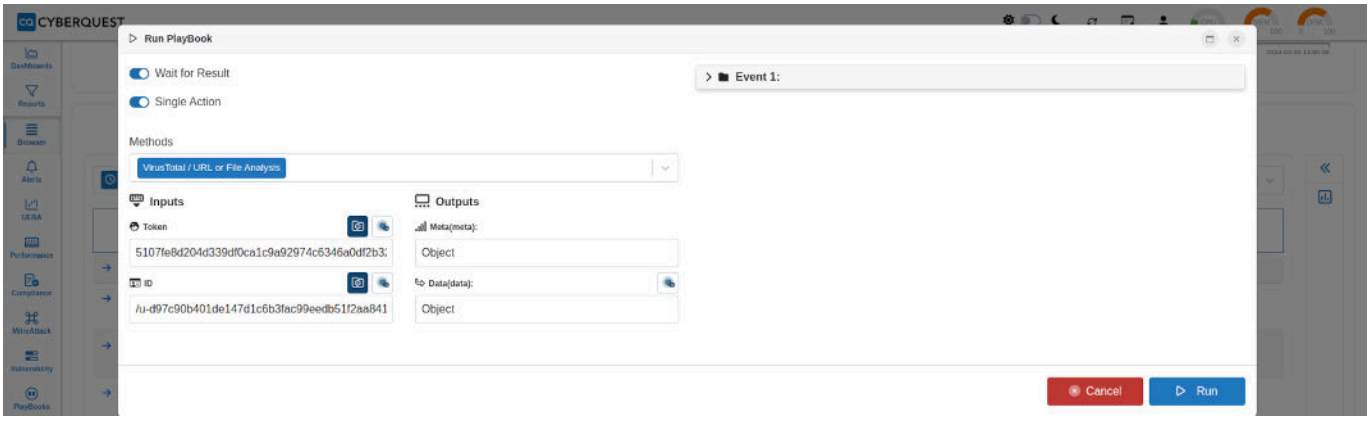


Inputs	Description
Token (is required)	To use the VirusTotal API, you must have an API key.
ID (is required)	The comment ID
Data (is required)	Vote type

Outputs	Description
Data (data)	The results of the API call

VirusTotal/URL or File Analysis method

Get a URL/file analysis.

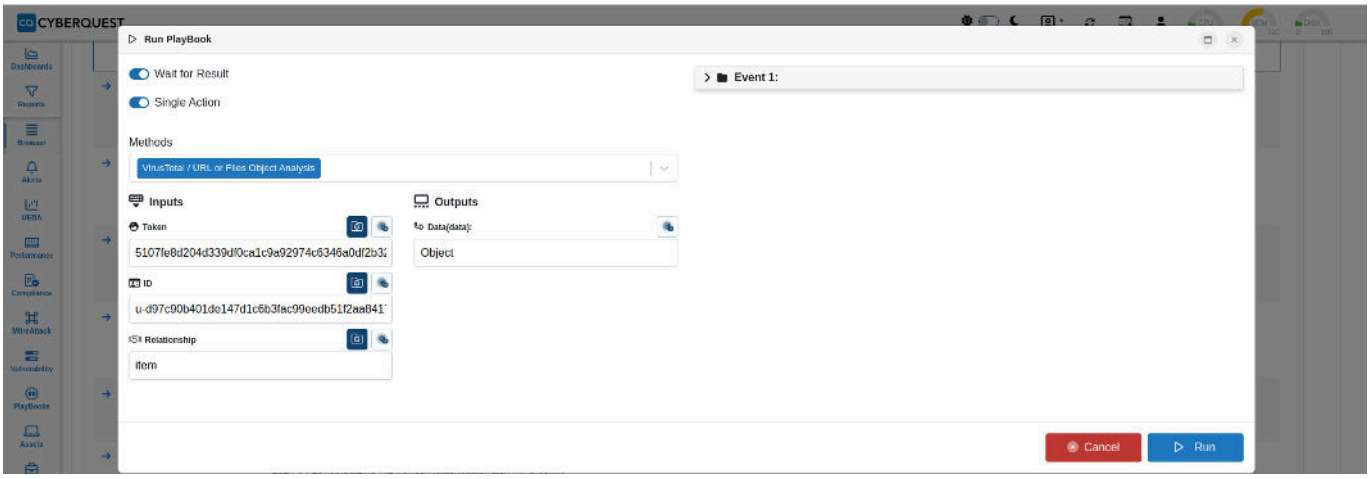


Inputs	Description
Token (is required)	To use the VirusTotal API, you must have an API key.
ID (is required)	The ID of the URL File which is investigated

Outputs	Description
Meta (meta)	Additional details
Data (data)	Indicates whether the analysis conducted on the data resulted in a harmless or non-threatening outcome, suggesting no presence of malicious or harmful elements.

VirusTotal/URL or Files Object Analysis method

Get objects related to an analysis.

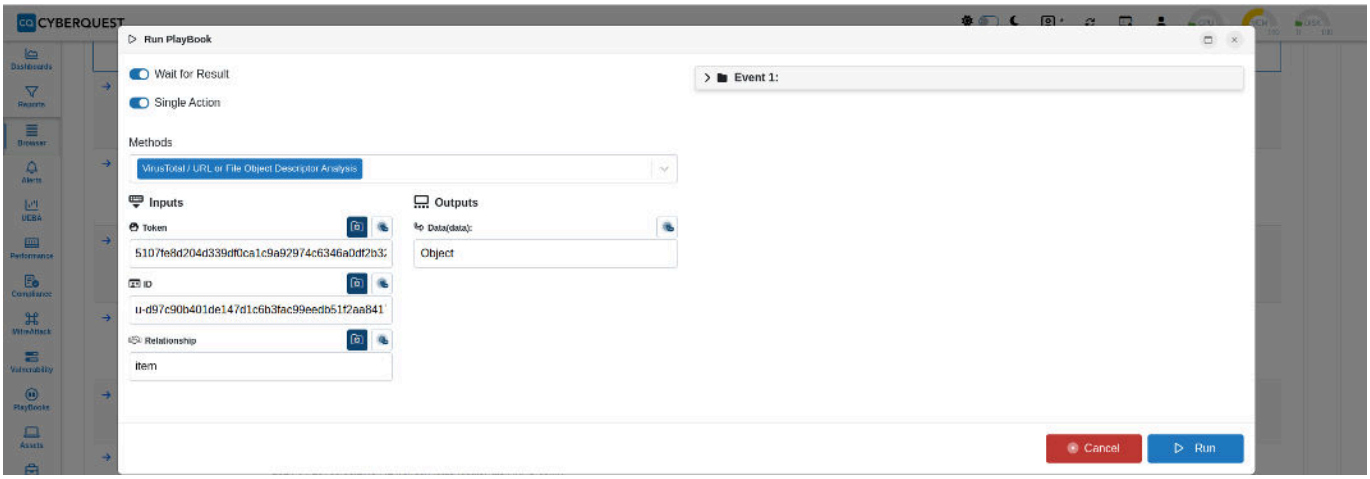


Inputs	Description
Token (is required)	To use the VirusTotal API, you must have an API key.
ID (is required)	The ID of the URL File which is investigated
Relationship (is required)	Relationship name

Outputs	Description
Data (data)	The results of the API call

VirusTotal/URL or File Object Descriptor Analysis method

Get object descriptors related to an analysis.

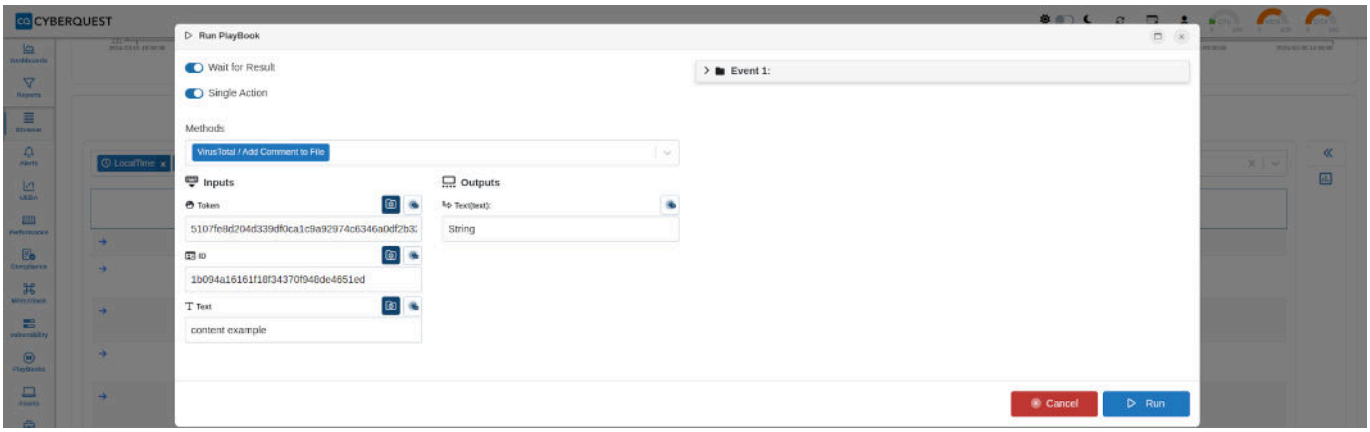


Inputs	Description
Token (is required)	To use the VirusTotal API, you must have an API key.
ID (is required)	The ID of the URL File which is investigated
Relationship (is required)	Relationship name

Outputs	Description
Data (data)	The results of the API call

VirusTotal/Add Comment to File method

Add a comment to a file.

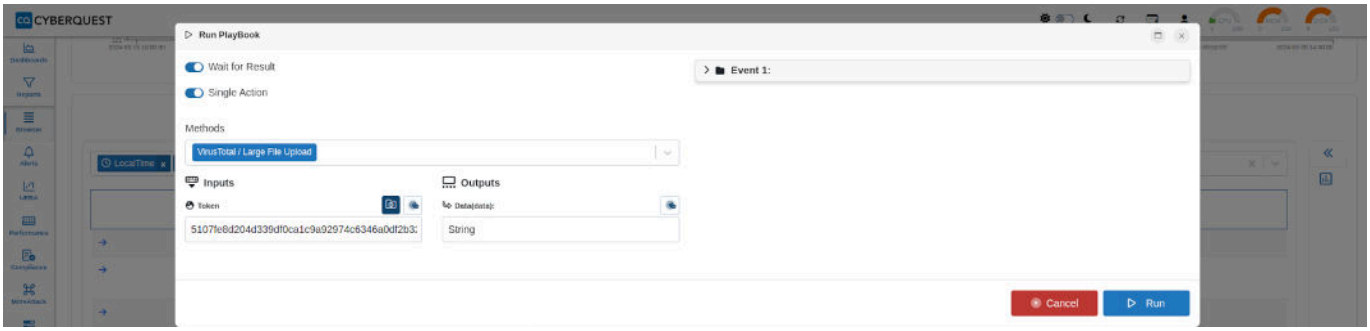


Inputs	Description
Token (is required)	To use the VirusTotal API, you must have an API key.
ID (is required)	The ID of the file which is investigated
Text (is required)	The content of the comment added to file

Outputs	Description
Data (data)	The results of the API call

VirusTotal/Large File Upload method

Get a URL for uploading large files.

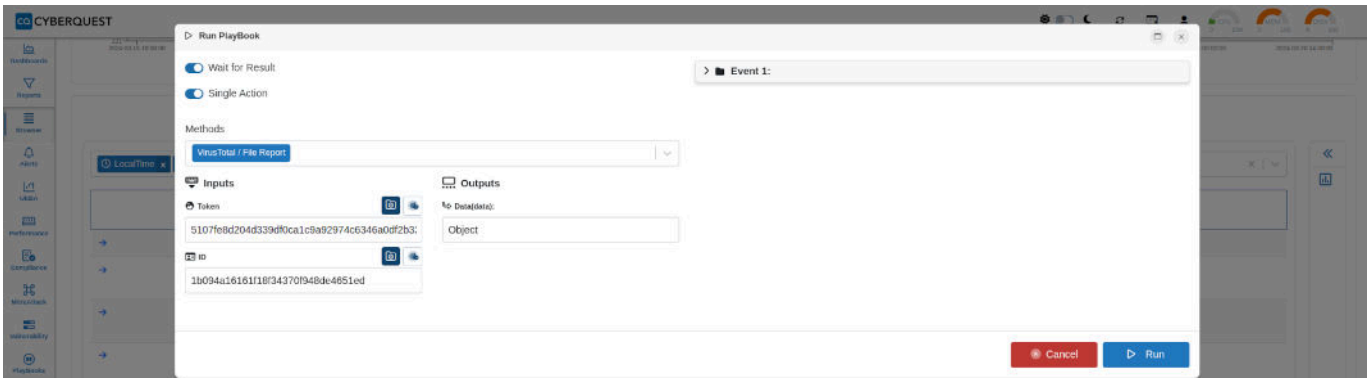


Inputs	Description
Token (is required)	To use the VirusTotal API, you must have an API key.

Outputs	Description
Data (data)	The link to upload a larger file

VirusTotal/File Report method

Get a file report.

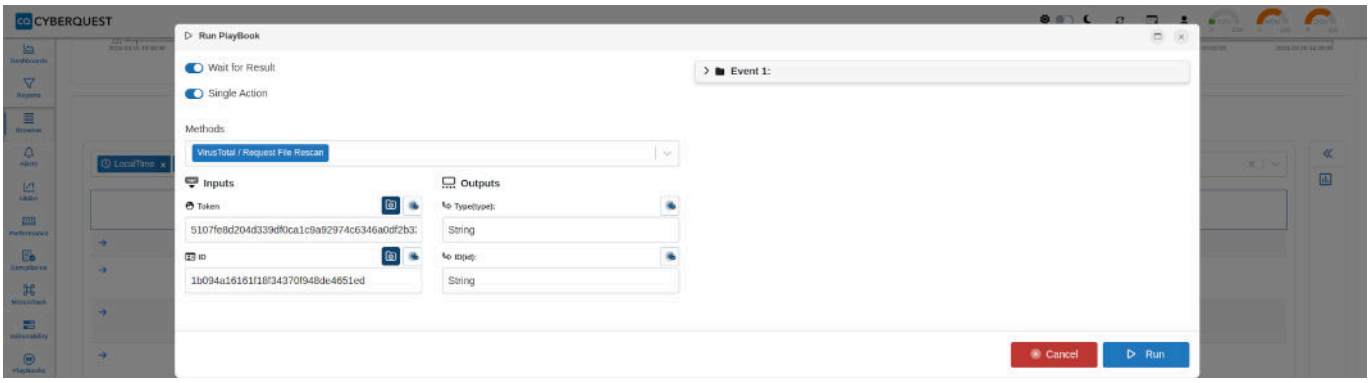


Inputs	Description
Token (is required)	To use the VirusTotal API, you must have an API key.
ID (is required)	The ID of the file which is investigated

Outputs	Description
Data (data)	The results of the API call

VirusTotal/Request File Rescan method

Request a file rescan.

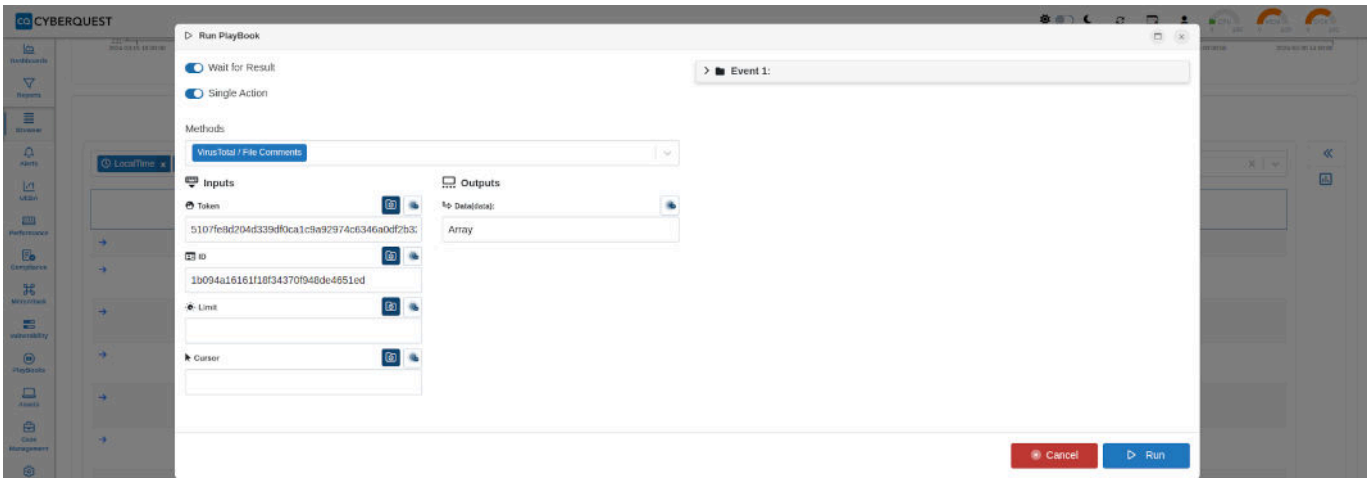


Inputs	Description
Token (is required)	To use the VirusTotal API, you must have an API key.
ID (is required)	The ID of the file which is investigated

Outputs	Description
Type (type)	The type of action
ID (id)	The new ID of file which is reanalyzed

VirusTotal/File Comments method

Get file comments.

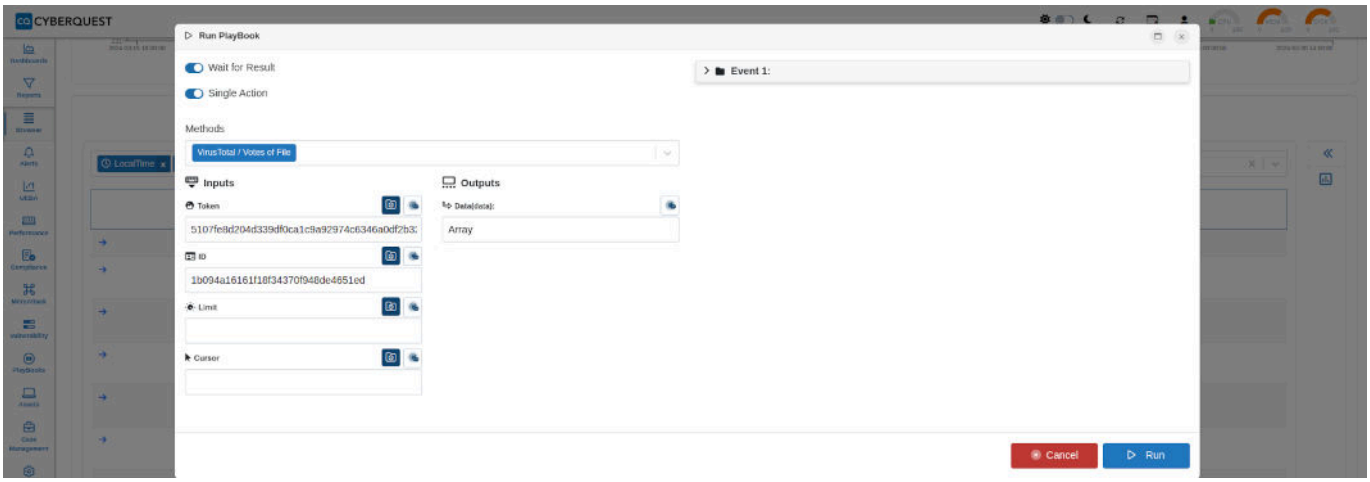


Inputs	Description
Token (is required)	To use the VirusTotal API, you must have an API key.
ID (is required)	The ID of the file which is investigated
Limit	Maximum number of related objects to retrieve
Cursor	Continuation cursor

Outputs	Description
Data (data)	A list with file comments

VirusTotal/Votes of File method

Get votes on a file.

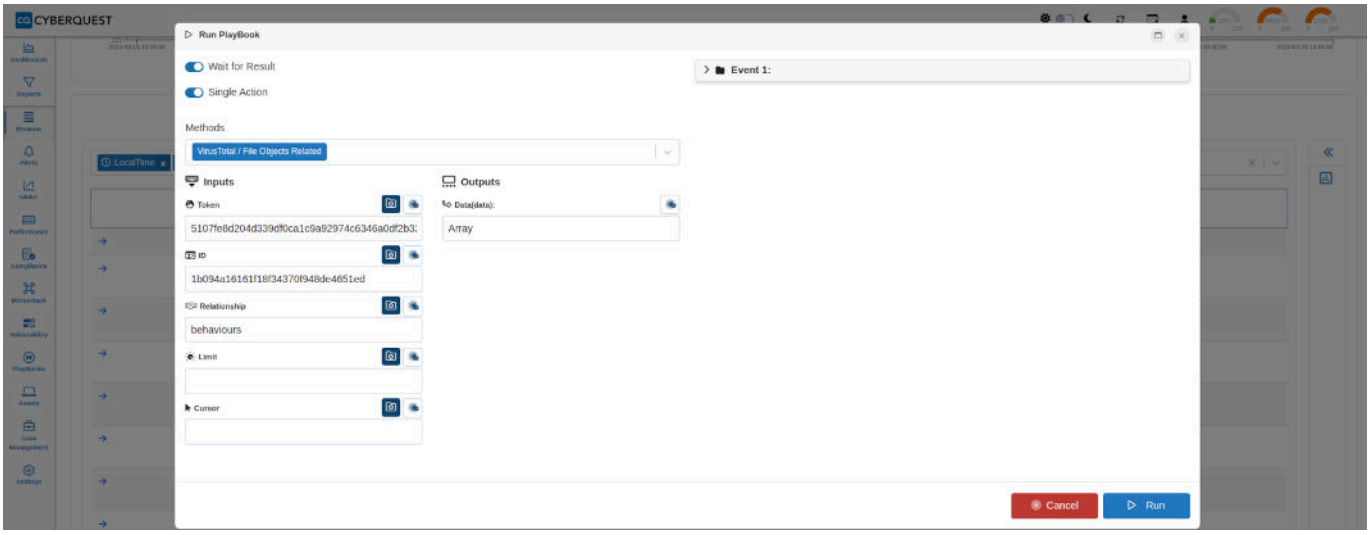


Inputs	Description
Token (is required)	To use the VirusTotal API, you must have an API key.
ID (is required)	The ID of the file which is investigated
Limit	Maximum number of related objects to retrieve
Cursor	Continuation cursor

Outputs	Description
Data (data)	A list with the votes of file which is investigated

VirusTotal/File Objects Related method

Get objects related to a file.

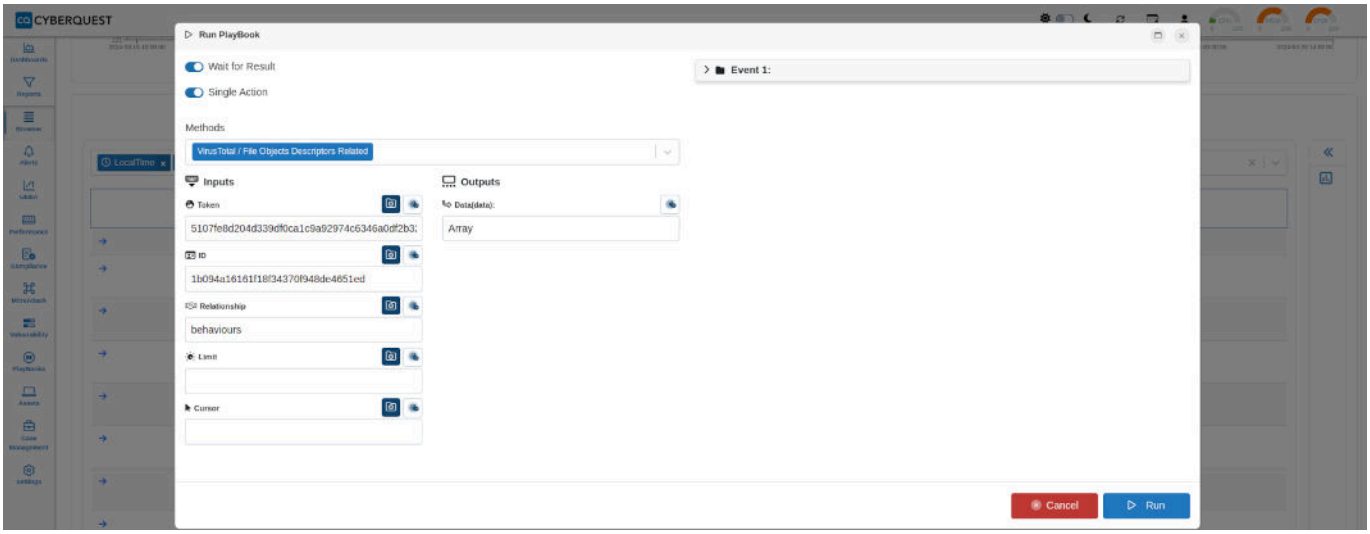


Inputs	Description
Token (is required)	To use the VirusTotal API, you must have an API key.
ID (is required)	The ID of the file which is investigated
Relationship (is required)	Relationship name
Limit	Maximum number of related objects to retrieve
Cursor	Continuation cursor

Outputs	Description
Data (data)	A list of File Objects Related

VirusTotal/File Objects Descriptors Related method

Get object descriptors related to a file.

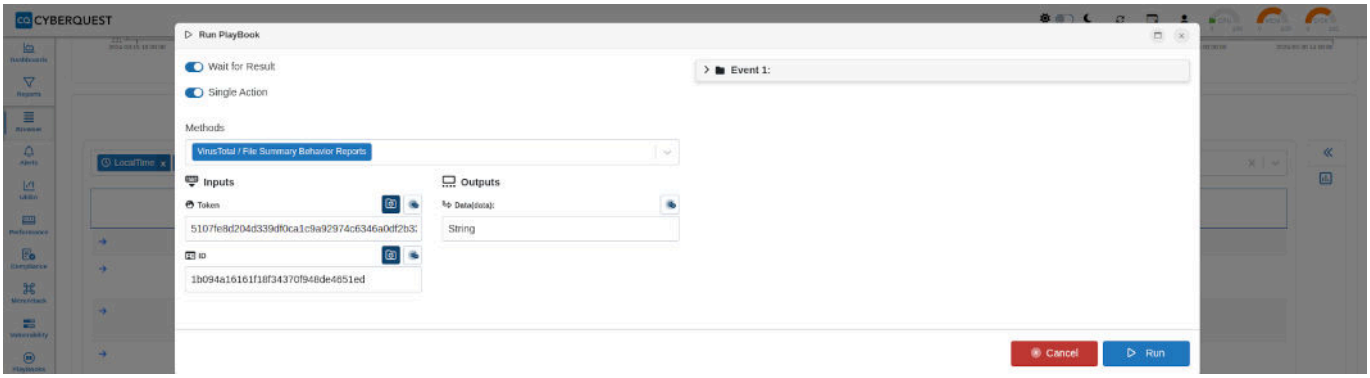


Inputs	Description
Token (is required)	To use the VirusTotal API, you must have an API key.
ID (is required)	The ID of the file which is investigated
Relationship (is required)	Relationship name
Limit	Maximum number of related objects to retrieve
Cursor	Continuation cursor

Outputs	Description
Data (data)	File Objects Descriptors Related

VirusTotal/File Summary Behavior Reports method

Get a summary of all behavior reports for a file.

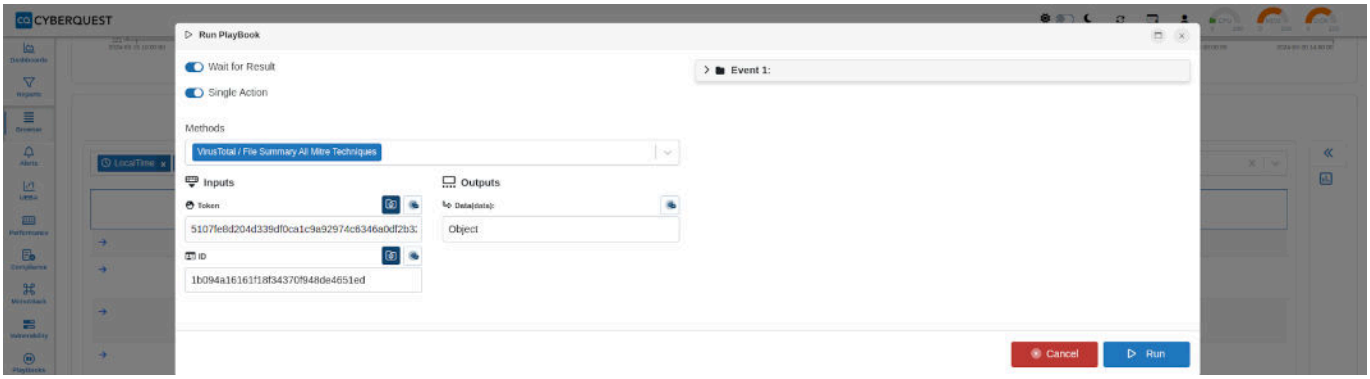


Inputs	Description
Token (is required)	To use the VirusTotal API, you must have an API key.
ID (is required)	The ID of the file which is investigated

Outputs	Description
Data (data)	Behavior Reports

VirusTotal/File Summary All Mitre Techniques method

Get a summary of all MITRE ATT&CK techniques observed in a file.

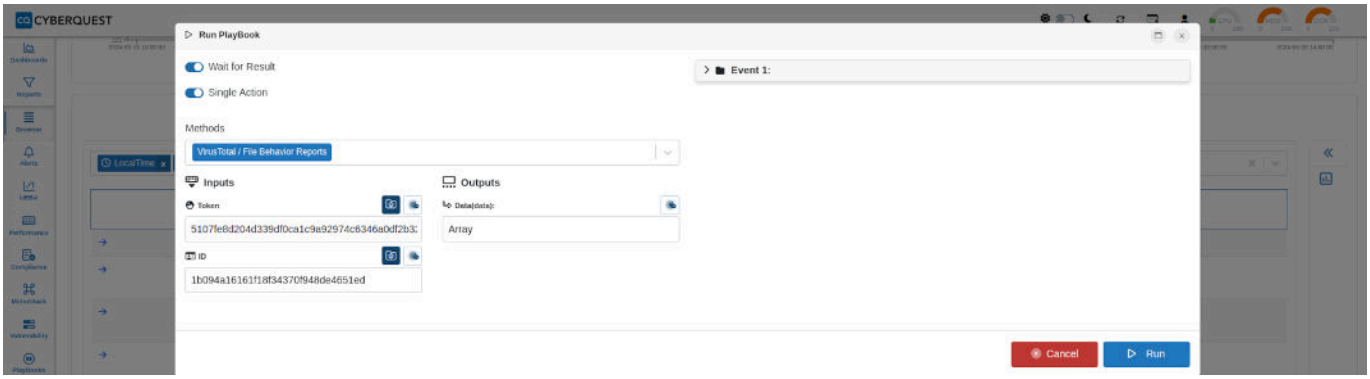


Inputs	Description
Token (is required)	To use the VirusTotal API, you must have an API key.
ID (is required)	The ID of the file which is investigated

Outputs	Description
Data (data)	All Mitre Techniques seen in file

VirusTotal/File Behavior Reports method

Get all behavior reports for a file.

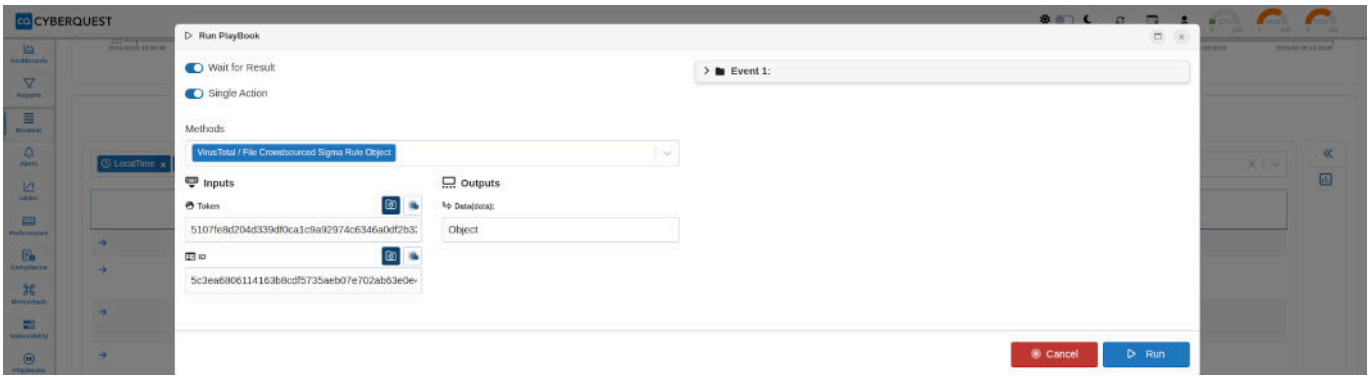


Inputs	Description
Token (is required)	To use the VirusTotal API, you must have an API key.
ID (is required)	The ID of the file which is investigated

Outputs	Description
Data (data)	Behavior Reports

VirusTotal/File Crowdsourced Sigma Rule Object method

Get a Crowdsourced Sigma rule object.

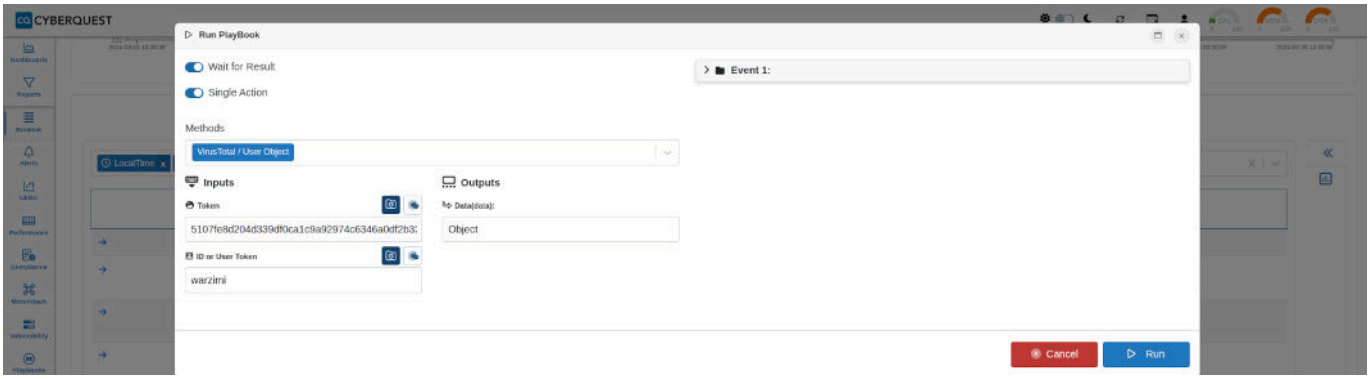


Inputs	Description
Token (is required)	To use the VirusTotal API, you must have an API key.
ID (is required)	The ID of the file which is investigated

Outputs	Description
Data (data)	The results of the API call

VirusTotal/User Object method

This endpoint retrieves information about a user, including the privileges and quotas associated to the user.

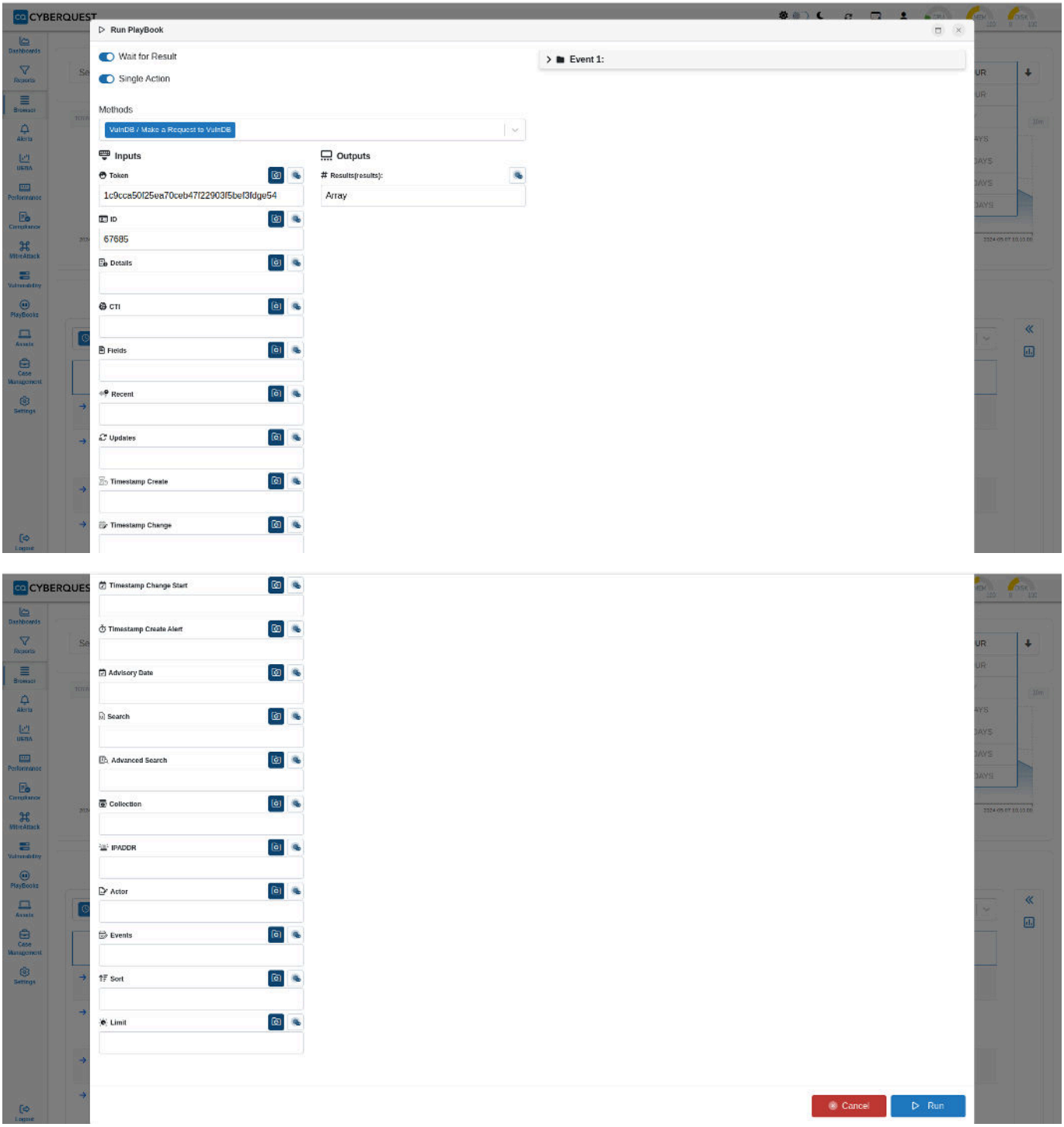


Inputs	Description
Token (is required)	To use the VirusTotal API, you must have an API key.
ID or User Token (is required)	User identification element

Outputs	Description
Data (data)	The results of the API call

VulnDB/Make a Request to VulnDB method

Get informations about: vulnerabilities, vendors, products (based on what parameters are provided).


CYBERQUEST
Run PlayBook
Wait for Result
Single Action
Methods
VulnDB / Make a Request to VulnDB
Inputs
Token
1c9cca50f25ea70ceb47f22903f5bef3fdge54
ID
67685
Details
CTI
Fields
Recent
Updates
Timestamp Create
Timestamp Change
Outputs
Results(results):
Array
Event 1:
Timestamp Change Start
Timestamp Create Alert
Advisory Date
Search
Advanced Search
Collection
IPADDR
Actor
Events
Sort
Limit
Cancel
Run

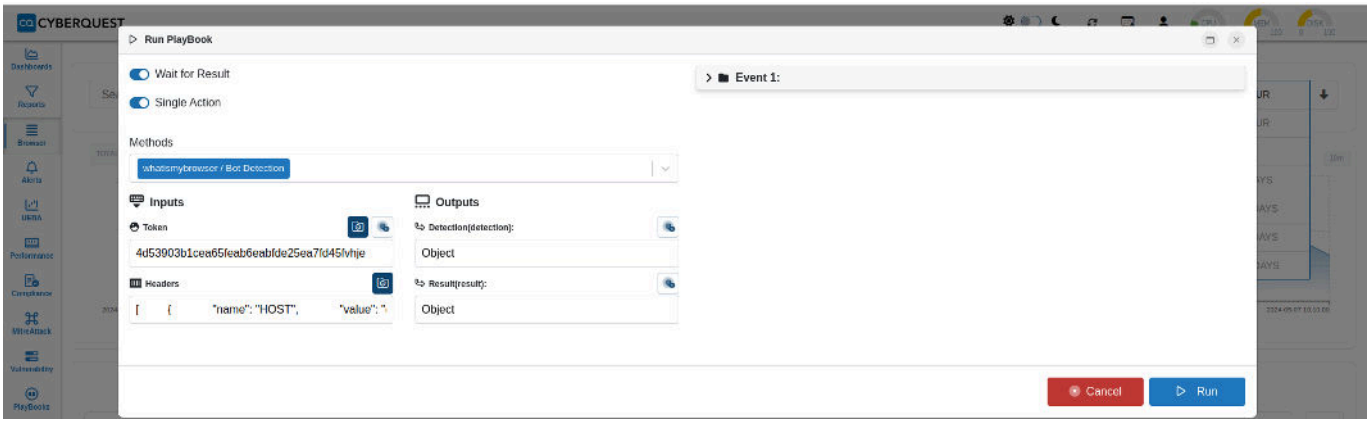
Inputs	Description
Token (is required)	To use the Vuldb API, you must have an API key.
ID	Vulnerability ID
Details	Show details about vulnerabilities
CTI	CTI (Cyber Threat Intelligence) to show information within API
Fields	This parameter is used if you want additional details
Recent	most recent entries
Updates	last updated
Timestamp Create	VulDB entry added to the database
Timestamp Change	VulDB entry changed for the last time
Timestamp Change Start	VulDB entry changed for the last time started
Timestamp Create Alert	VulDB entry added to the database stated
Advisory Date	VulDB advisory start date
Search	state search queries like they would be used in a search on the web site.
Advanced Search	The field can hold multiple search keys
Collection	Predefined set of entries. This is often used as vendor or product-based collections within streamlined vulnerability management handling
IPADDR	Query IP address to get risk level
Actor	APT actor names
Events	possible current events
Sort	For sorting response
Limit	For limiting responses

Outputs	Description
Results (results)	The results of the API call

WhatIsMyBrowser

whatismybrowser/Bot Detection method

Detect the requesting software/agent.



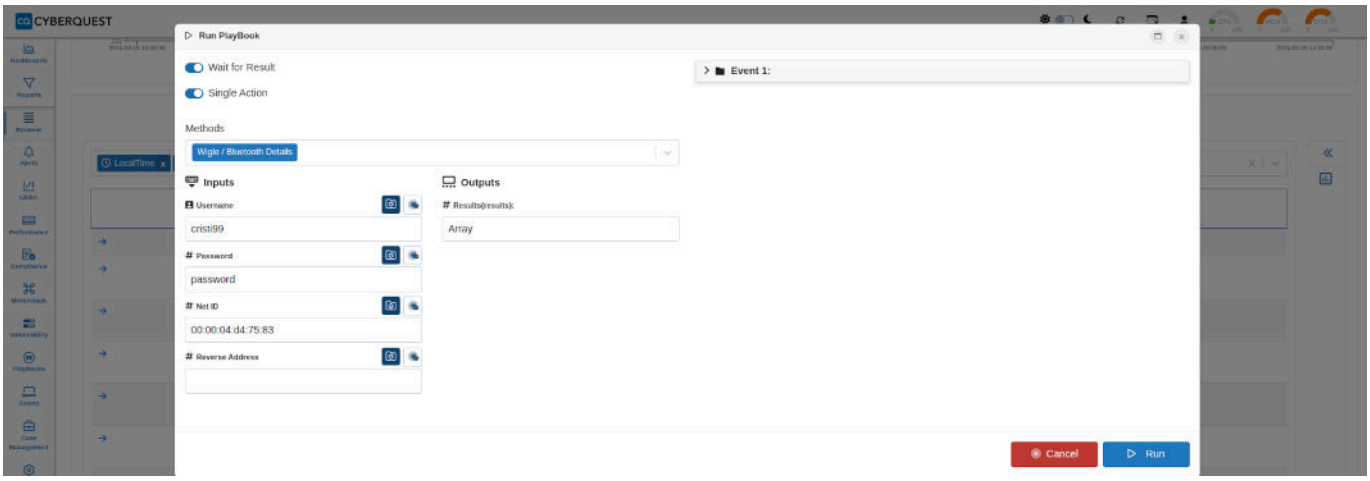
Inputs	Description
Token (is required)	To use the WhatIsMyBrowser API, you must have an API key.
Headers (is required)	The HTTP headers send by the visitors

Outputs	Description
Detection (detection)	The results of the API call
Result (result)	The status of the API call

Wigle

Wigle/Bluetooth Details method

Provide unique information for a Bluetooth network. API and session authentication default to a page size of 100 results/page. Number of daily queries allowed per user are throttled based on history and participation. Detail endpoints are NOT included in COMMAPI subscriptions at this time.

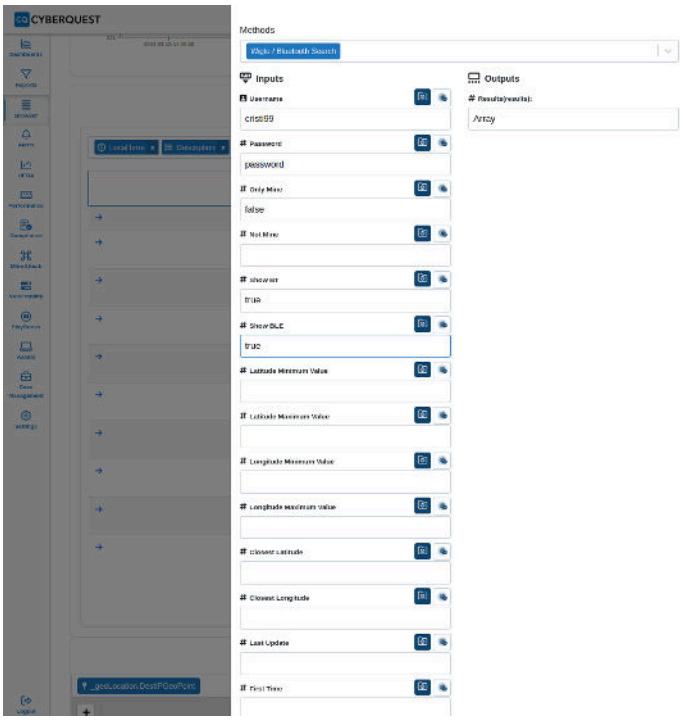


Inputs	Description
Username (is required)	Username from Wigle Account
Password (is required)	The Password from Wigle Account
Net ID (is required)	The full Bluetooth Device ID to search
Reverse Address	Reverse geocode for an approximate address

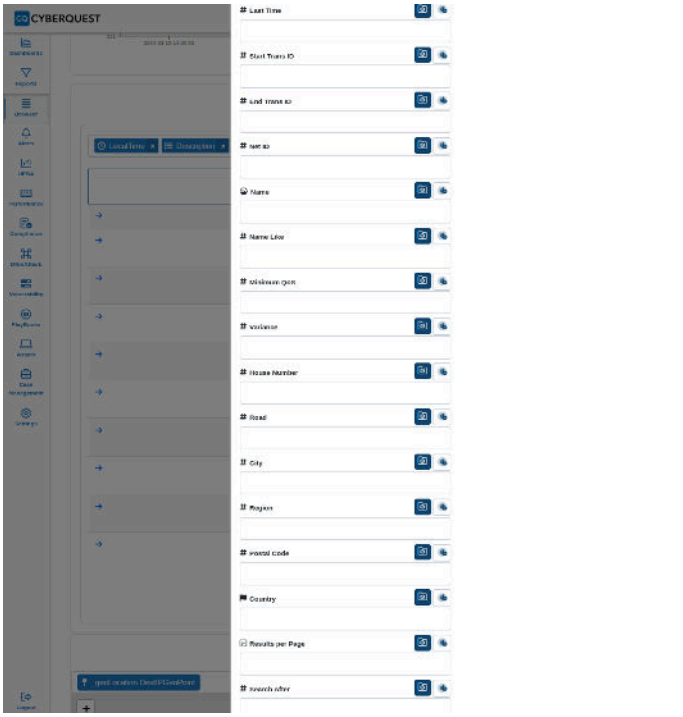
Outputs	Description
Results (results)	The results of the API call

Wigle/Bluetooth Search method

Provide unique information for a Bluetooth network. API and session authentication default to a page size of 100 results/page. Number of daily queries allowed per user are throttled based on history and participation. Detail endpoints are NOT included in COMMAPI subscriptions at this time.


CYBERQUEST
Methods
Inputs
Outputs
Username
cris899
Password
password
Only Mine
false
Not Mine
true
Show BLE
true
Latitude Minimum Value
Latitude Maximum Value
Longitude Minimum Value
Longitude maximum Value
Closest Latitude
Closest Longitude
Last Update
First Time
Array


EVENTID


CYBERQUEST
Last Time
Start Trans ID
Name
Name Line
House Number
Road
City
Region
Postal code
Country
Results per Page

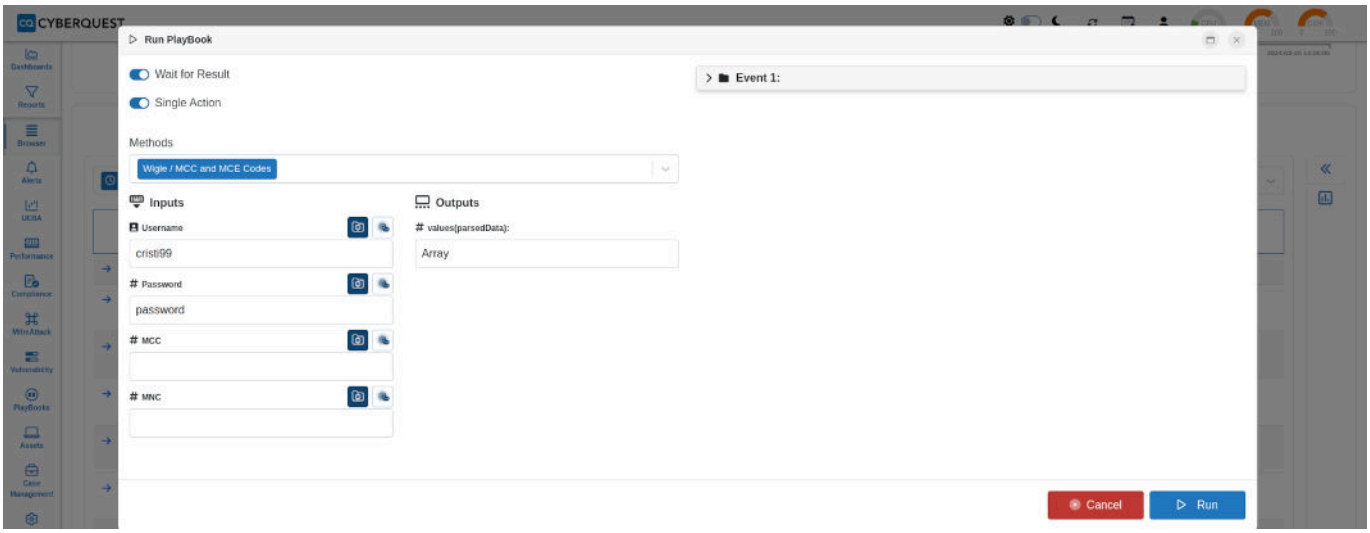

EVENTID

Inputs	Description
Username (is required)	Username from Wigle Account
Password (is required)	The Password from Wigle Account
Only Mine	Search only for points first discovered by the current user.
Not Mine	Only search for networks first seen by other users
Show BT	Include BT networks
Show BLE	Include BLE networks
Latitude Minimum Value	Lesser of two latitudes by which to bound the search (specify both)
Latitude Maximum Value	Greater of two latitudes by which to bound the search (specify both)
Longitude Minimum Value	Lesser of two longitudes by which to bound the search (specify both)
Longitude Maximum Value	Greater of two longitudes by which to bound the search (specify both)
Closest Latitude	Latitude to order by closest network (requires closestLong)
Closest Longitude	Longitude to order by closest network (requires closestLat)
Last Update	Filter points by how recently theyve been updated (more recent than this value), condensed date/time numeric string format yyyyMMdd[hhmm[ss]]
First Time	Filter points by when they were first created (more recent than this value), condensed date/time numeric string format yyyyMMdd[hhmm[ss]]
Last Time	Filter points by how recently theyve had data submitted (more recent than this value), condensed date/time numeric string format yyyyMMdd[hhmm[ss]]
Start Trans ID	Earliest transid by which to bound (year-level precision only), format yyyyMMdd-00000
End Trans ID	Latest transid by which to bound (year-level precision only), format yyyyMMdd-00000
Net ID	Include only networks matching the string network BSSID, e.g. 0A:2C:EF:3D:25:1B or 0A:2C:EF. The first three octets are required.
Name	Include only networks exactly matching the string network name.
Name Like	Include only networks matching the string network name, allowing wildcards % (any string) and _ (any character).
Minimum QoS	Minimum Quality of Signal
Variance	How tightly to bound queries against the provided latitude/longitude box. Value must be between 0.001 and 0.2. Intended for use with non-exact decimals and geocoded bounds.
House Number	Street address house number
Road	Street address road
City	Street address city
Region	Street address region
Postal Code	Street address postal code
Country	Street address country
Results per Page	How many results to return per request. Defaults to 25 for COMMAPI, 100 for site. Bounded at 1000 for COMMAPI, 100 for site.
Search After	Put in the previous pages searchAfter result to get the next page. Use this instead of first

Outputs	Description
Results (results)	The results of the API call

Wigle/MCC and MCE Codes method

Get MCC and MNC codes for Cellular Networks.

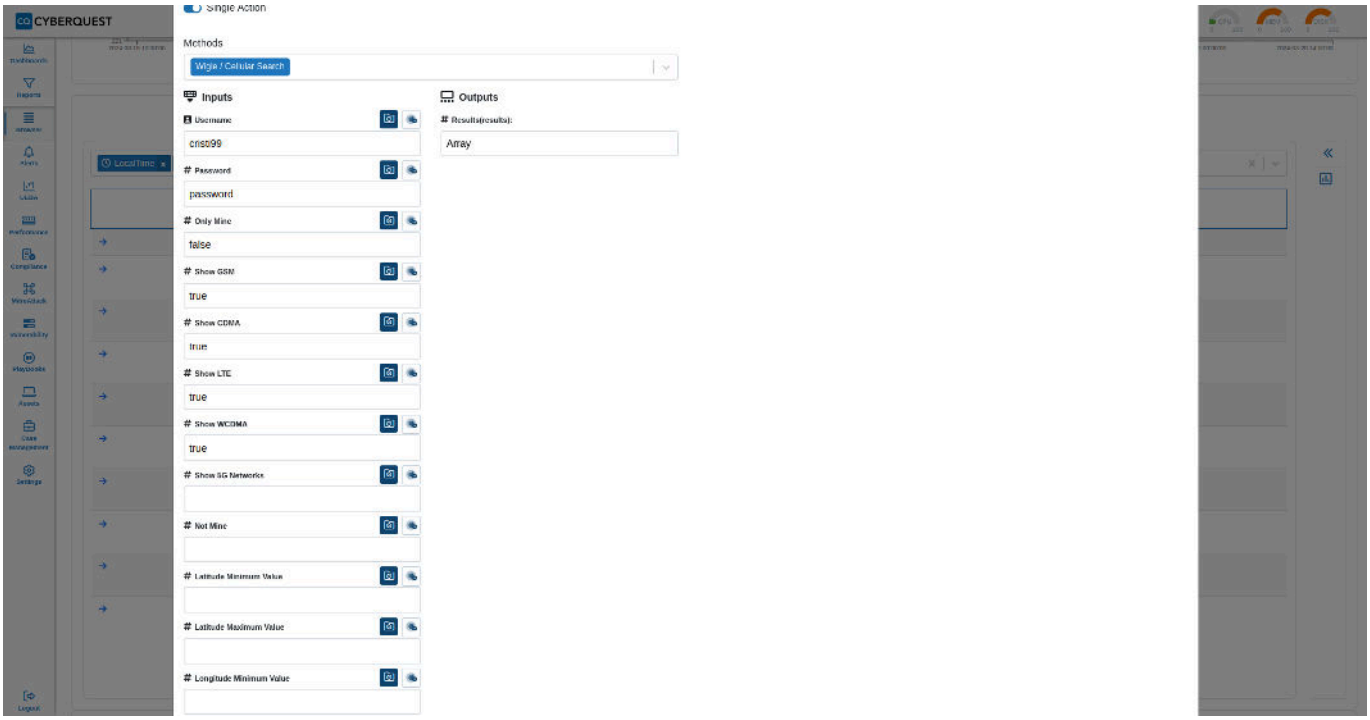


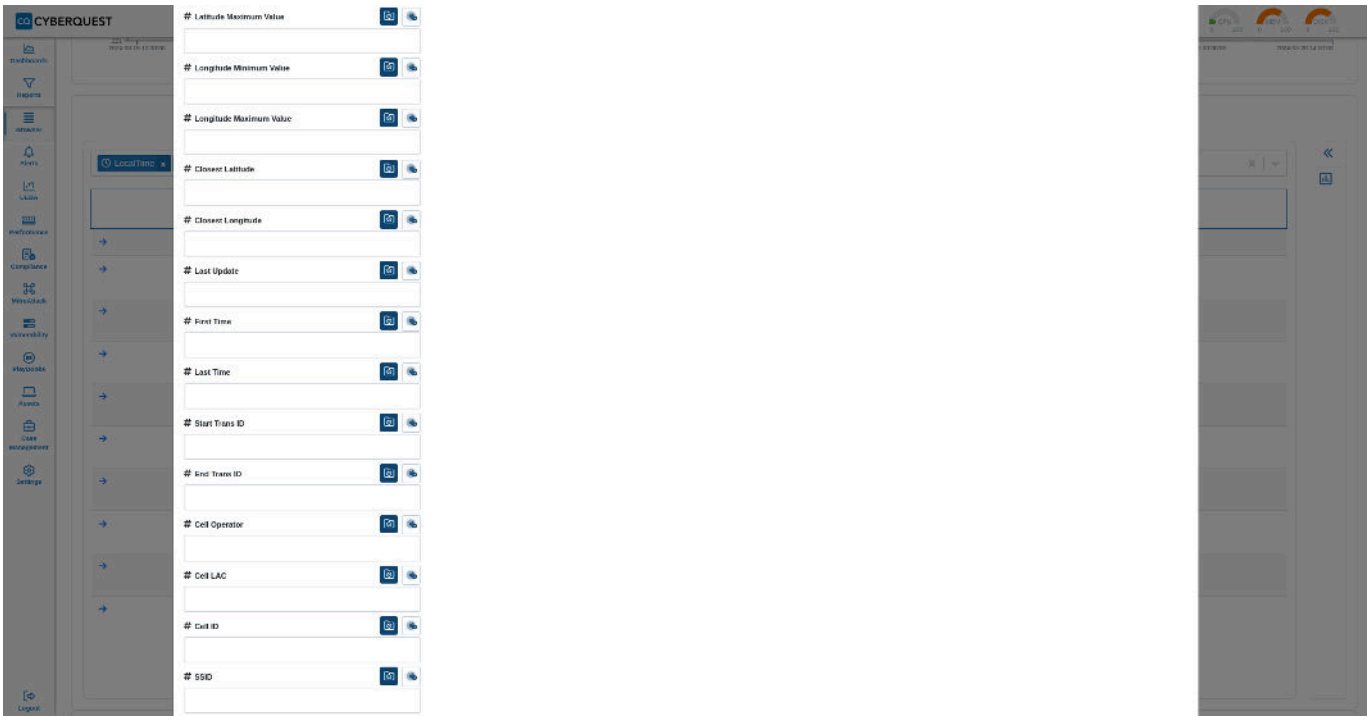
Inputs	Description
Username (is required)	Username from Wigle Account
Password (is required)	The Password from Wigle Account
MCC	MCC (Mobile Country Code) to filter
MNC	MNC (Mobile Network Code) to filter

Outputs	Description
values (parsedData)	The results of the API call

Wigle/Cellular Search method

Search the WIGLE database.


CYBERQUEST
Single Action
Methods
Wigle / Cellular Search
Inputs
Outputs
Username
cristi99
Password
password
Only Mine
false
Show GSM
true
Show CDMA
true
Show LTE
true
Show WCDMA
true
Show 5G Networks
Not Mine
Latitude Minimum Value
Latitude Maximum Value
Longitude Minimum Value
Result(results):
Array


CYBERQUEST
Latitude Maximum Value
Longitude Minimum Value
Longitude Maximum Value
Closest Latitude
Closest Longitude
Last Update
First Time
Last Time
Start Trans ID
End Trans ID
Cell Operator
Cell LAC
Cell ID
SSID


SSID Like
Minimum QoS
Variance
House Number
Road
City
Region
Postal Code
Country
Results per Page
Search After
Cancel
Run

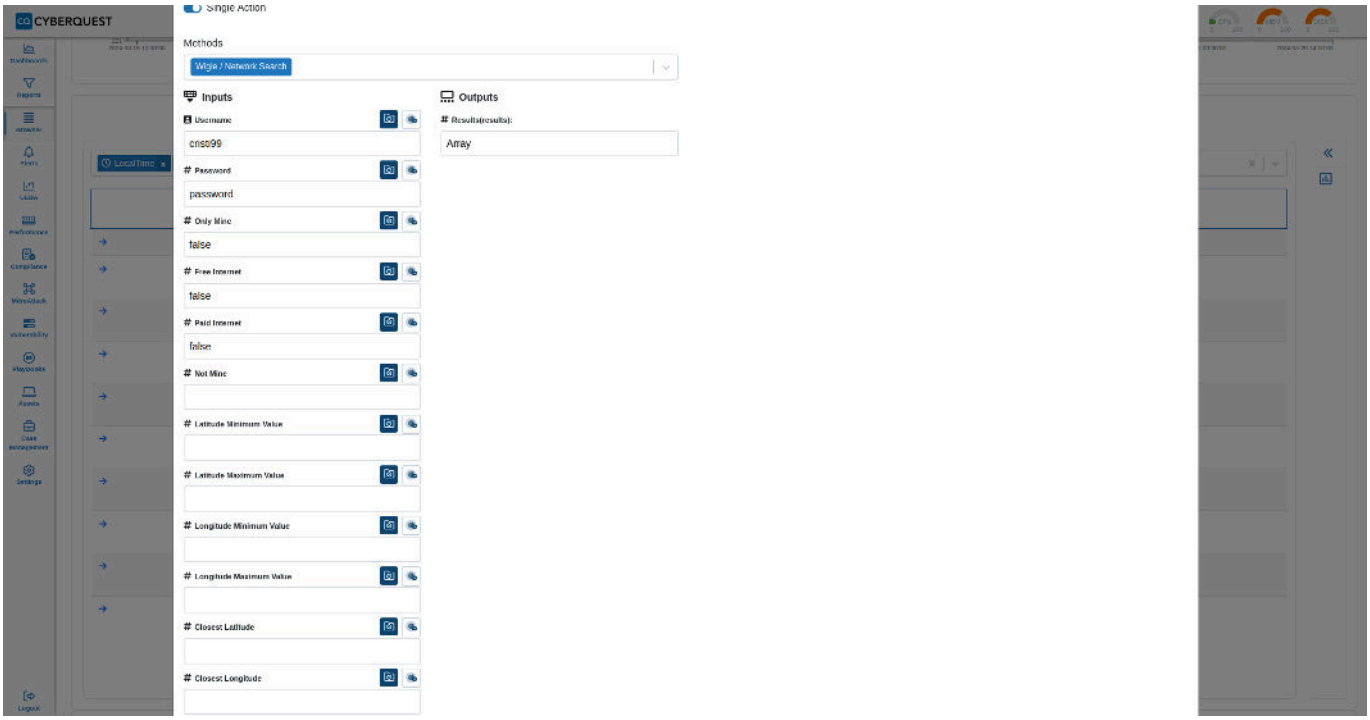
Inputs	Description
Username (is required)	Username from Wigle Account
Password (is required)	The Password from Wigle Account
Only Mine	Search only for points first discovered by the current user.
Show GSM	Include GSM cell networks
Show CDMA	Include CDMA cell networks
Show LTE	Include LTE cell networks
Show WCDMA	Include WCDMA cell networks
Show 5G Networks	Include 5G NR cell networks
Not Mine	Only search for networks first seen by other users
Latitude Minimum Value	Lesser of two latitudes by which to bound the search (specify both)
Latitude Maximum Value	Greater of two latitudes by which to bound the search (specify both)
Longitude Minimum Value	Lesser of two longitudes by which to bound the search (specify both)
Longitude Maximum Value	Greater of two longitudes by which to bound the search (specify both)
Closest Latitude	Search only for points first discovered by the current user.
Closest Longitude	Longitude to order by closest network (requires closestLat)
Last Update	Filter points by how recently theyve been updated (more recent than this value), condensed date
First Time	Filter points by when they were first created (more recent than this value), condensed date/time numeric string format yyyyMMdd[hhmm[ss]]
Last Time	Filter points by how recently theyve had data submitted (more recent than this value), condensed date
Start Trans ID	Earliest transid by which to bound (year-level precision only), format yyyyMMdd-00000
End Trans ID	Latest transid by which to bound (year-level precision only), format yyyyMMdd-00000
Cell Operator	Cell Operator (GSM/LTE/WCDMA/5G NR) or System (CDMA) ID parameter by which to filter
Cell LAC	Cell LAC (Local Area Code) (GSM/LTE/WCDMA/5G NR) or Network (CDMA) ID parameter by which to filter
Cell ID	Cell ID(GSM/LTE/WCDMA/5G NR) or Basestation (CDMA) parameter by which to filter
SSID	Include only cell towers exactly matching the string network name.
SSID Like	Include only cell towers matching the string network name, allowing wildcards % (any string) and _ (any character).
Minimum QoS	Minimum Quality of Signal
Variance	How tightly to bound queries against the provided latitude/longitude box. Value must be between 0.001 and 0.2. Intended for use with non-exact decimals and geocoded bounds.
House Number	Street address house number
Road	Street address road
City	Street address city
Region	Street address region
Postal Code	Street address postal code
Country	Street address country

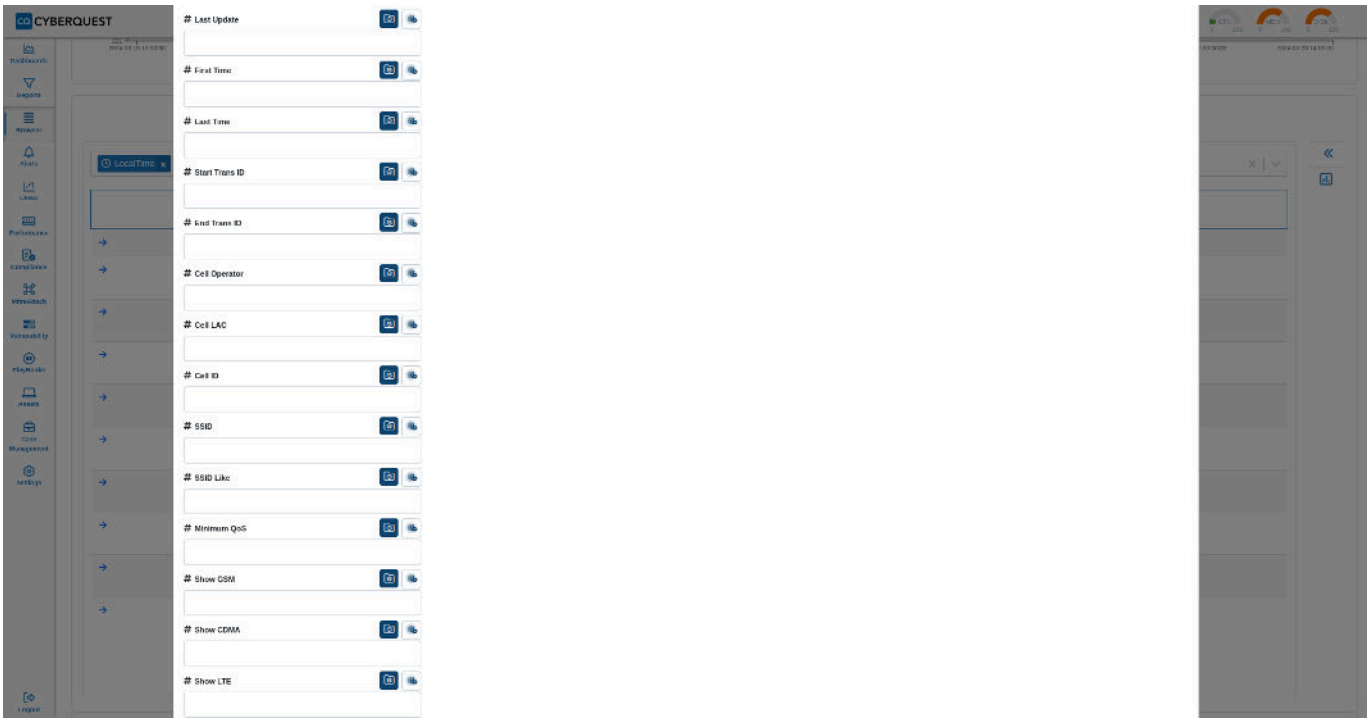
Inputs	Description
Results per Page	How many results to return per request. Defaults to 25 for COMMAPI, 100 for site. Bounded at 1000 for COMMAPI, 100 for site.
Search After	Put in the previous pages searchAfter result to get the next page. Use this instead of first

Outputs	Description
Results (results)	The results of the API call

Wigle/Network Search method

Search the Wigle Cell database.






Show WCDMA
Show 5G Networks
Variance
House Number
Road
City
Region
Postal Code
Country
Results per Page
Search After
Cancel
Run

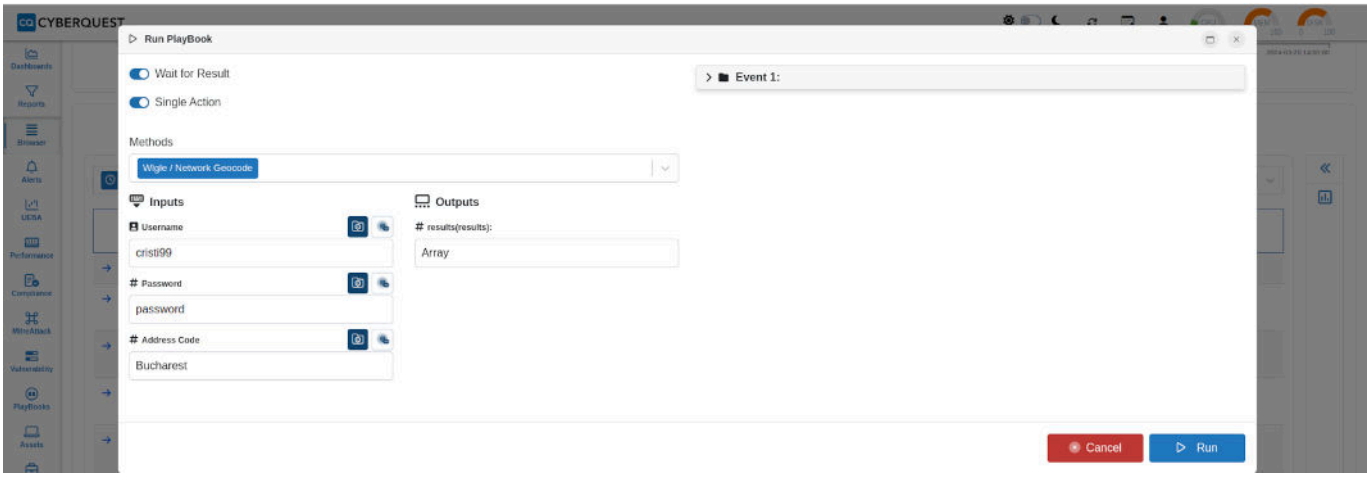
Inputs	Description
Username (is required)	Username from Wigle Account
Password (is required)	The Password from Wigle Account
Only Mine	Search only for points first discovered by the current user.
Free Internet	Include only networks that have been marked as free access.
Paid Internet	Include only networks that have been marked as for-pay access.
Not Mine	Only search for networks first seen by other users
Latitude Minimum Value	Lesser of two latitudes by which to bound the search (specify both)
Latitude Maximum Value	Greater of two latitudes by which to bound the search (specify both)
Longitude Minimum Value	Lesser of two longitudes by which to bound the search (specify both)
Longitude Maximum Value	Greater of two longitudes by which to bound the search (specify both)
Closest Latitude	Search only for points first discovered by the current user.
Closest Longitude	Longitude to order by closest network (requires closestLat)
Last Update	Filter points by how recently theyve been updated (more recent than this value), condensed date
First Time	Filter points by when they were first created (more recent than this value), condensed date/time numeric string format yyyyMMdd[hhmm[ss]]
Last Time	Filter points by how recently theyve had data submitted (more recent than this value), condensed date
Start Trans ID	Earliest transid by which to bound (year-level precision only), format yyyyMMdd-00000
End Trans ID	Latest transid by which to bound (year-level precision only), format yyyyMMdd-00000
Cell Operator	Cell Operator (GSM/LTE/WCDMA/5G NR) or System (CDMA) ID parameter by which to filter
Cell LAC	Cell LAC (Local Area Code) (GSM/LTE/WCDMA/5G NR) or Network (CDMA) ID parameter by which to filter
Cell ID	Cell ID(GSM/LTE/WCDMA/5G NR) or Basestation (CDMA) parameter by which to filter
SSID	Include only cell towers exactly matching the string network name.
SSID Like	Include only cell towers matching the string network name, allowing wildcards % (any string) and _ (any character).
Minimum QoS	Minimum Quality of Signal
Show GSM	Include GSM cell networks
Show CDMA	Include CDMA cell networks
Show LTE	Include LTE cell networks
Show WCDMA	Include WCDMA cell networks
Show 5G Networks	Include 5G NR cell networks
Variance	How tightly to bound queries against the provided latitude/longitude box. Value must be between 0.001 and 0.2. Intended for use with non-exact decimals and geocoded bounds.
House Number	Street address house number
Road	Street address road
City	Street address city
Region	Street address region

Inputs	Description
Postal Code	Street address postal code
Country	Street address country
Results per Page	How many results to return per request. Defaults to 25 for COMMAPI, 100 for site. Bounded at 1000 for COMMAPI, 100 for site.
Search After	Put in the previous pages searchAfter result to get the next page. Use this instead of first

Outputs	Description
Results (results)	The results of the API call

Wigle/Network Geocode method

Get coordinates for an address for use in searching.

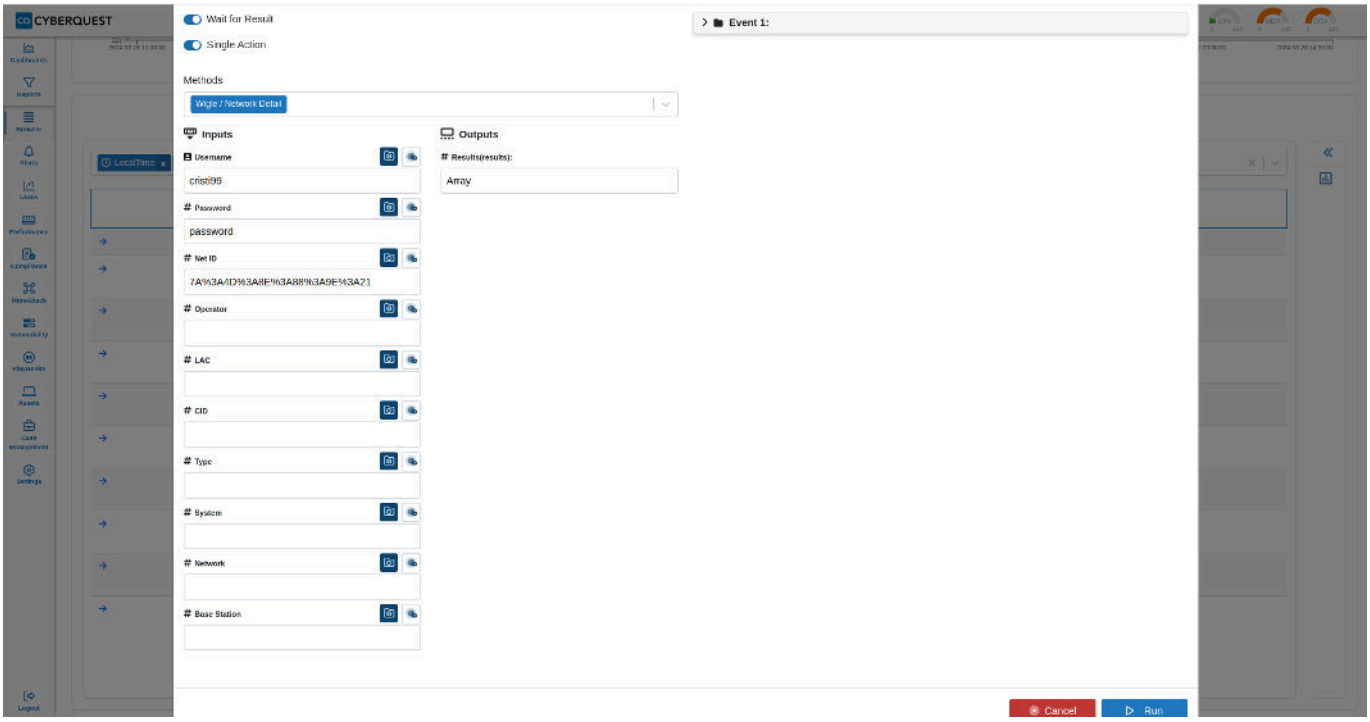


Inputs	Description
Username (is required)	Username from Wigle Account
Password (is required)	The Password from Wigle Account
Address Code (is required)	An address string, Street, City, State/Region, Country

Outputs	Description
results (results)	The results of the API call

Wigle/Network Detail method

Add a comment to a network.

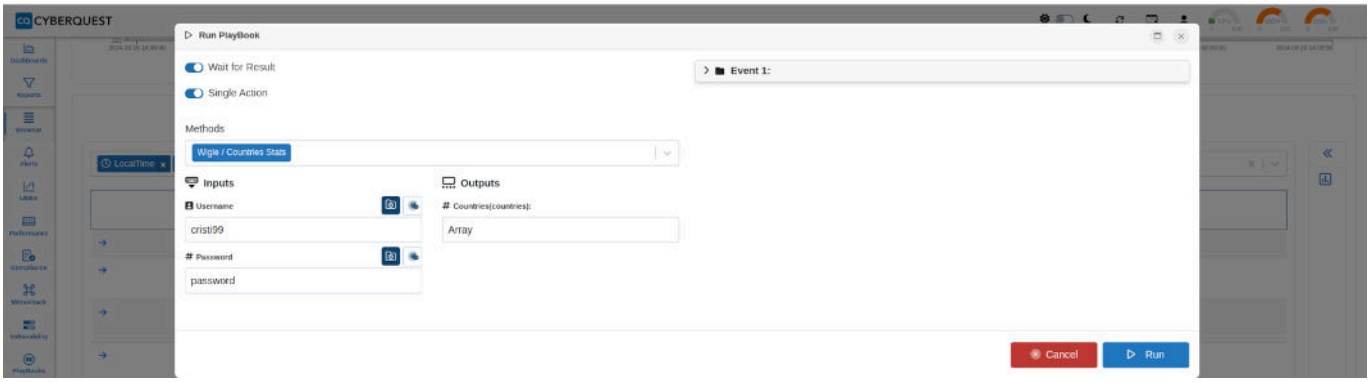


Inputs	Description
Username (is required)	Username from Wigle Account
Password (is required)	The Password from Wigle Account
Net ID	The WiFi Network BSSID to search
Operator	GSM/LTE/WCDMA/5G NR Operator ID
LAC	GSM/LTE/WCDMA/5G NR Location Area Code
CID	GSM/LTE/WCDMA/5G NR Cell ID/NIR
Type	Network Type: CDMA/GSM/LTE/WCDMA/NR/WIFI
System	CDMA System ID
Network	CDMA Network ID
Base Station	CDMA Base Station ID

Outputs	Description
Results (results)	The results of the API call

Wigle/Countries Stats method

Get statistics organized by country.

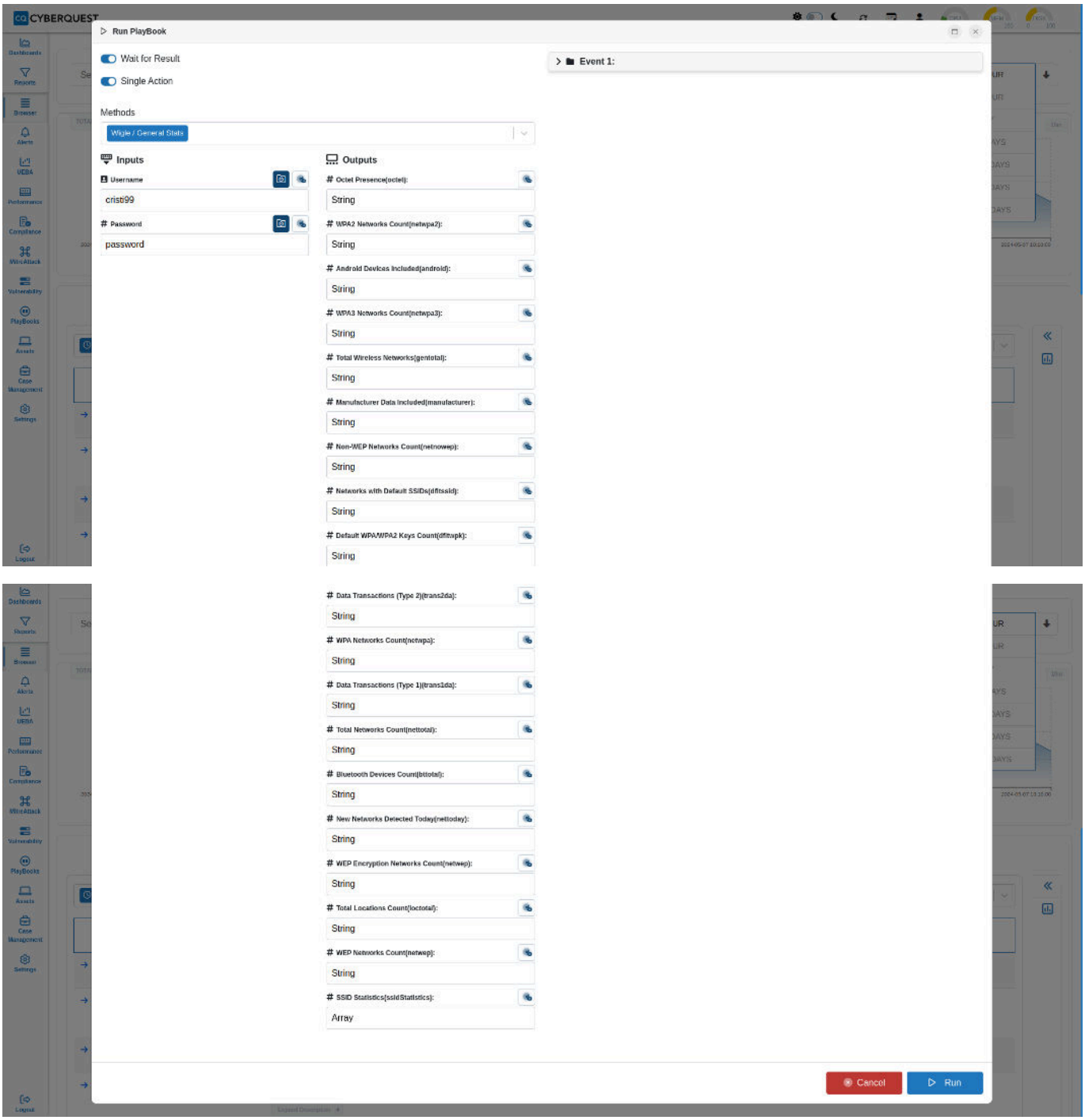


Inputs	Description
Username (is required)	Username from Wigle Account
Password (is required)	The Password from Wigle Account

Outputs	Description
Countries (countries)	The results of the API call

Wigle/General Stats method

Get a named map of general upload statistics.

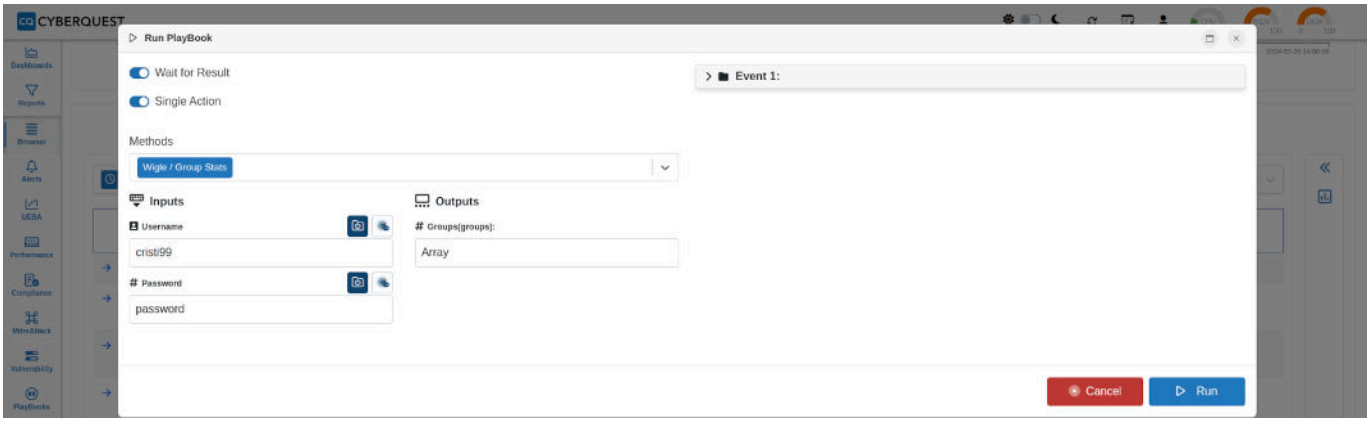


Inputs	Description
Username (is required)	Username from Wigle Account
Password (is required)	The Password from Wigle Account

Outputs	Description
Octet Presence (octet)	The number of Octet
WPA2 Networks Count (netwpa2)	The number of WPA2 Networks
Android Devices Included (android)	The number of Android Devices
WPA3 Networks Count (netwpa3)	The number of WPA3 Networks
Total Wireless Networks (gentotal)	The number of Total Wireless Networks
Manufacturer Data Included (manufacturer)	True if it includes data about manufacturers
Non-WEP Networks Count (netnowep)	The number of Non-WEP Networks
Networks with Default SSIDs (dfltssid)	The number of Networks with Default SSIDs
Default WPA/WPA2 Keys Count (dfltwpk)	The number of Default WPA/WPA2 Keys Count
Data Transactions (Type 2) (trans2da)	The number of Data Transactions (Type 2)
WPA Networks Count (netwpa)	The number of WPA Networks
Data Transactions (Type 1) (trans1da)	The number of Data Transactions (Type 1)
Total Networks Count (nettotal)	The number of Total Networks
Bluetooth Devices Count (bttotal)	The number of Bluetooth Devices
New Networks Detected Today (nettoday)	The number of New Networks Detected Today
WEP Encryption Networks Count (netwep)	The number of WEP Encryption Networks
Total Locations Count (loctotal)	The number of WEP Encryption Networks
WEP Networks Count (netwep)	The number of WEP Network
SSID Statistics (ssidStatistics)	Additional details about SSID Statistics

Wigle/Group Stats method

Get group standings.

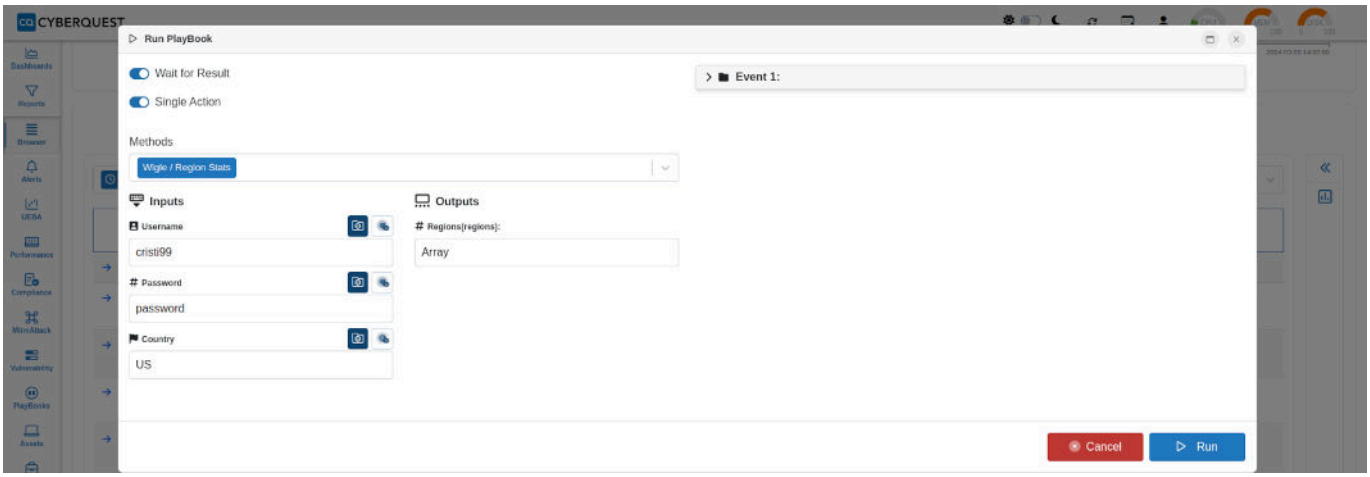


Inputs	Description
Username (is required)	Username from Wigle Account
Password (is required)	The Password from Wigle Account

Outputs	Description
Groups (groups)	The results of the API call

Wigle/Region Stats method

Get statistics for a specified country, organized by region, postal code and encryption.

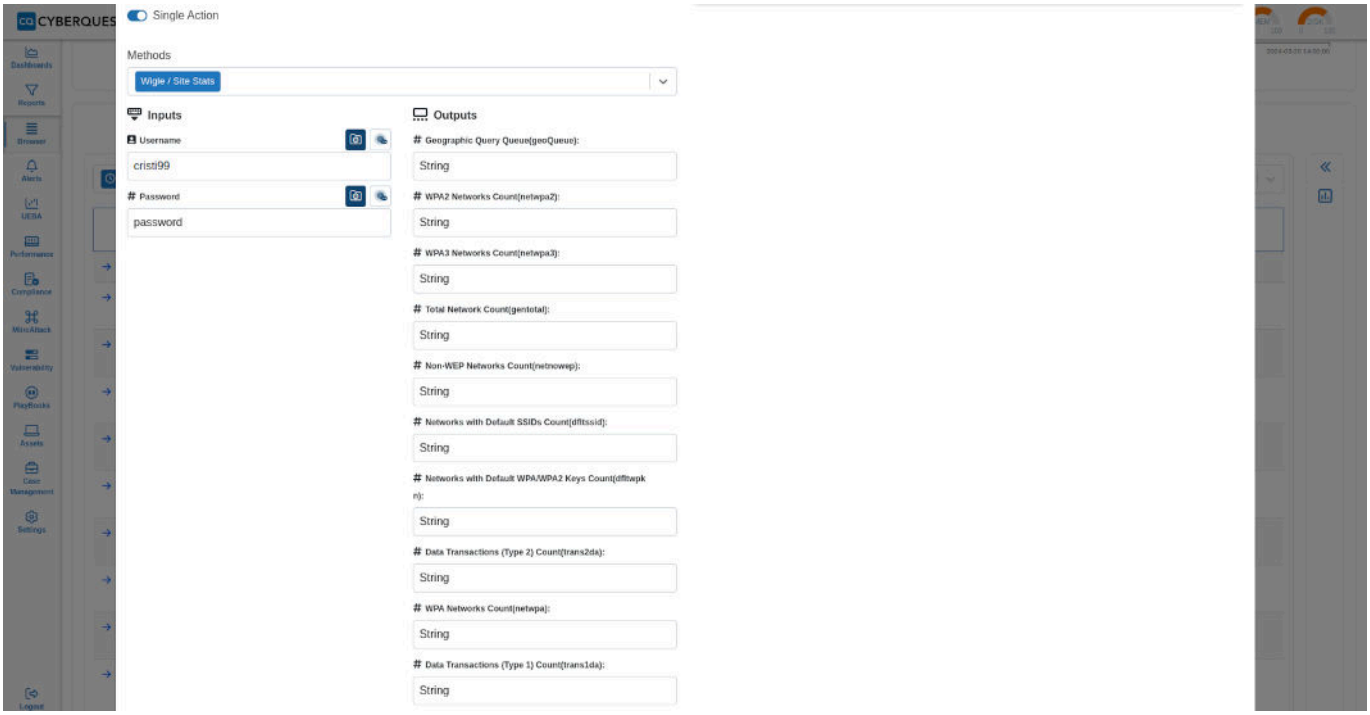


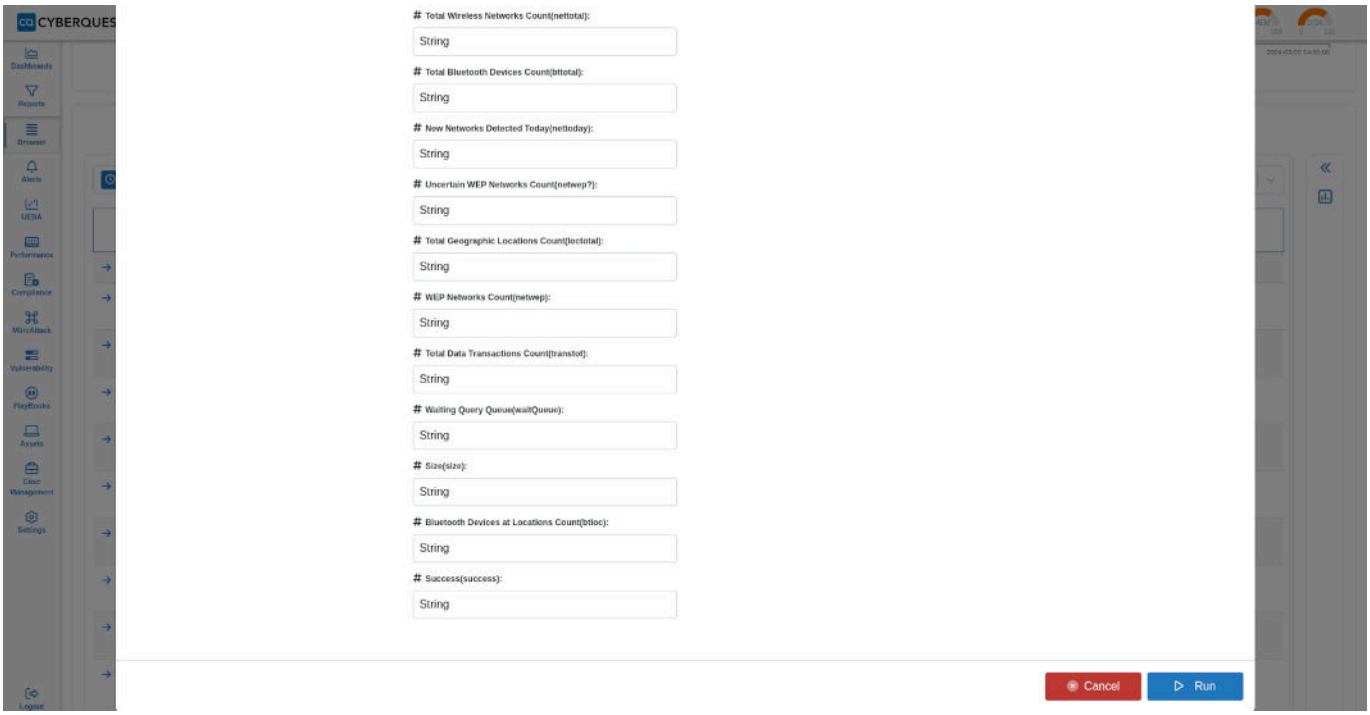
Inputs	Description
Username (is required)	Username from Wigle Account
Password (is required)	The Password from Wigle Account
Country (is required)	The two-letter code of the country for which youd like a regional breakdown. Defaults to US

Outputs	Description
Regions (regions)	The results of the API call

Wigle/Site Stats method

Get a named map of site-level statistics.



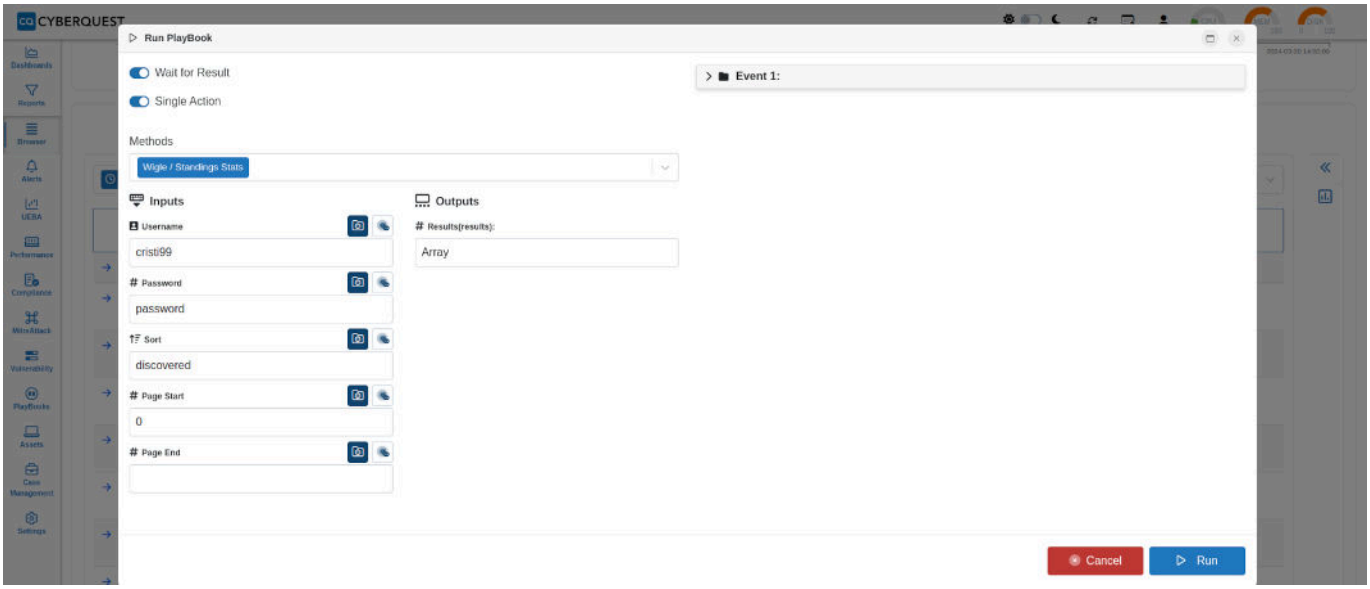


Inputs	Description
Username (is required)	Username from Wigle Account
Password (is required)	The Password from Wigle Account

Outputs	Description
Geographic Query Queue (geoQueue)	The number of Geographic Query Queue
WPA2 Networks Count (netwpa2)	The number of WPA2 Networks
WPA3 Networks Count (netwpa3)	The number of WPA3 Networks
Total Network Count (gentotal)	The number of Total Network
Non-WEP Networks Count (netnowep)	The number of Non-WEP Networks
Networks with Default SSIDs Count (dfltssid)	The number of Networks with Default SSID
Networks with Default WPA/WPA2 Keys Count (dfltwpkn)	The number of Networks with Default WPA/WPA2 Keys
Data Transactions (Type 2) Count (trans2da)	The number of Data Transactions (Type 2)
WPA Networks Count (netwpa)	The number of WPA Network
Data Transactions (Type 1) Count (trans1da)	The number of Data Transactions (Type 1)
Total Wireless Networks Count (nettotal)	The number of Total Wireless Networks
Total Bluetooth Devices Count (bttotal)	The number of Total Bluetooth Devices
New Networks Detected Today (nettoday)	The number of New Networks Detected
Uncertain WEP Networks Count (netwep?)	The number of Uncertain WEP Networks
Total Geographic Locations Count (loctotal)	The number of Total Geographic Locations
WEP Networks Count (netwep)	The number of WEP Networks Count
Total Data Transactions Count (transtot)	The number of Total Data Transactions
Waiting Query Queue (waitQueue)	The number of Waiting Query Queue
Size (size)	Size
Bluetooth Devices at Locations Count (btloc)	The number of Bluetooth Devices at Locations
Success (success)	True if the API call was successful

Wigle/Standings Stats method

Get user standings.

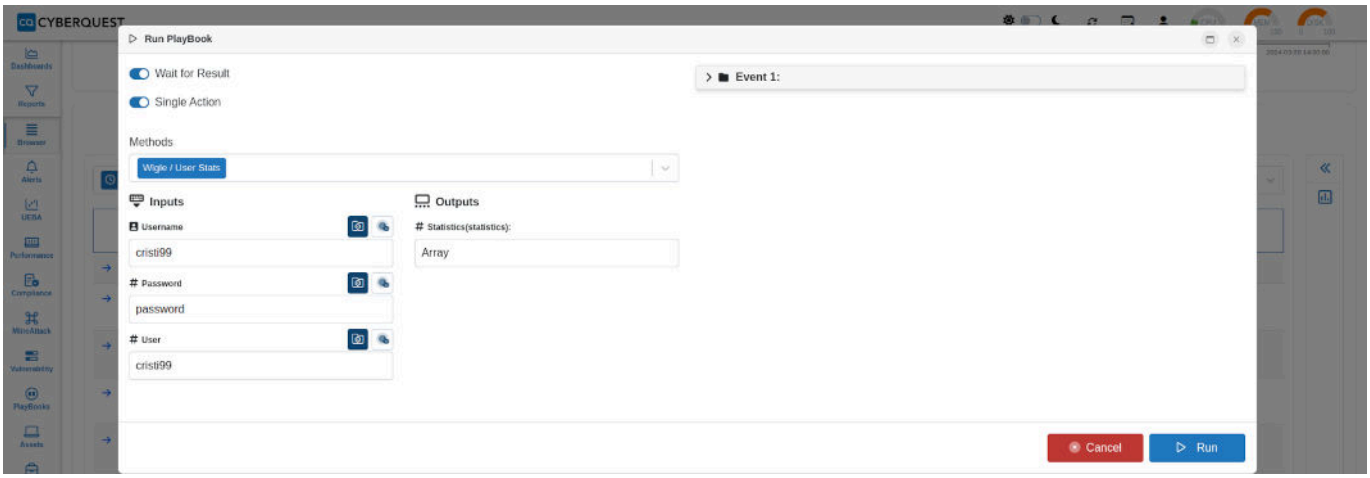


Inputs	Description
Username (is required)	Username from Wigle Account
Password (is required)	The Password from Wigle Account
Sort	The criteria by which to sort the results. Values are [discovered, total, monthcount, prevmonthcount, gendisc, gentotal, firsttransid, lasttransid]
Page Start	The first record to request according to the sort paramete
Page End	The last record to request according to the sort parameter

Outputs	Description
Results (results)	The results of the API call

Wigle/User Stats method

Get user statistics.



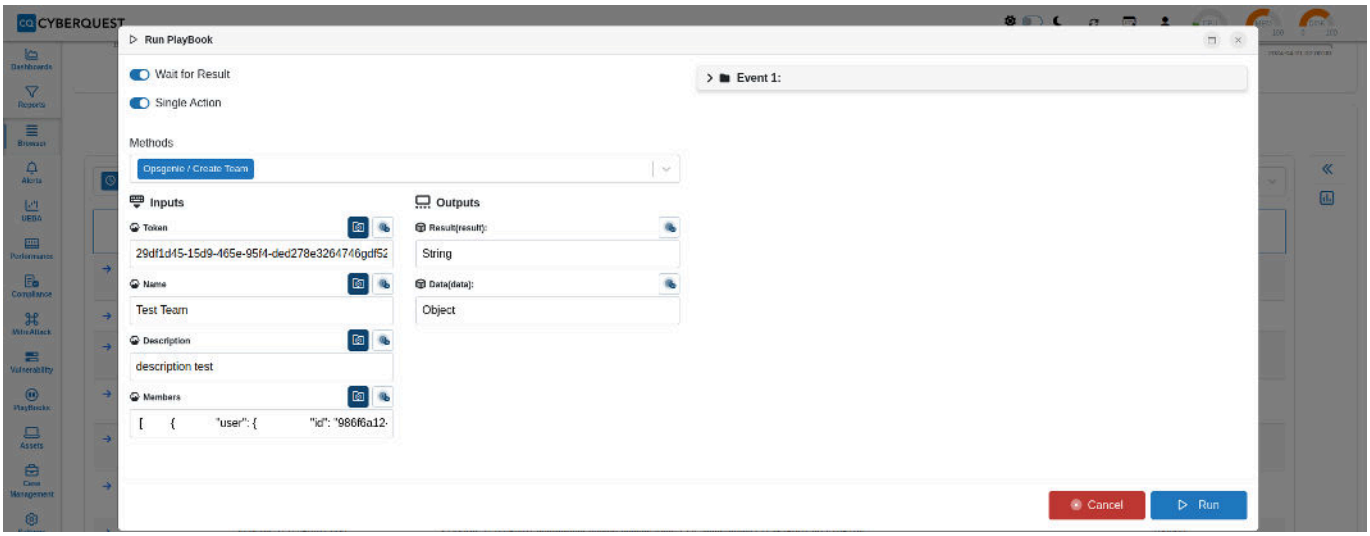
Inputs	Description
Username (is required)	Username from Wigle Account
Password (is required)	The Password from Wigle Account
User (is required)	The name of the user for whom to get stats

Outputs	Description
Statistics (statistics)	The results of the API call

Opsgenie

Opsgenie/Create Team method

Creates a new team.

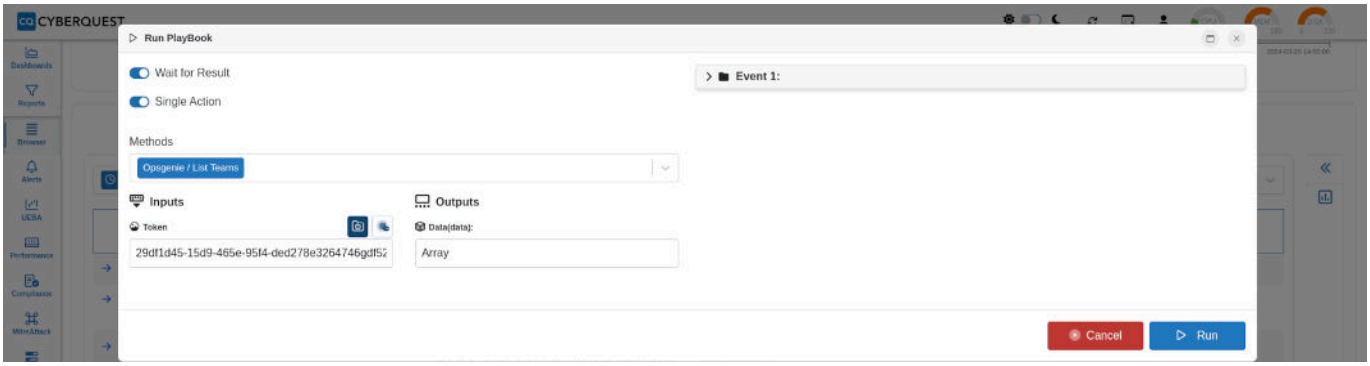


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Name (is required)	Name of the team
Description	The description of team
Members	The users which will be added to team, and optionally their roles.

Outputs	Description
Result (result)	The result of the API call
Data (data)	Details about the new created team

Opsgenie/List Teams method

Return list of teams.

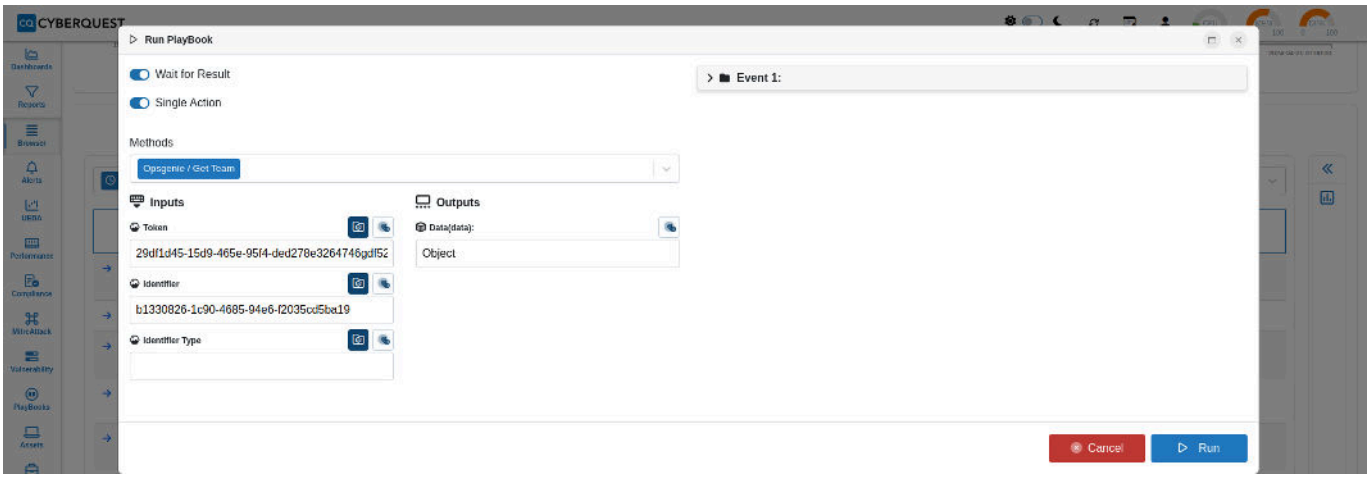


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.

Outputs	Description
Data (data)	The result of the API call

Opsgenie/Get Team method

Returns team with given id or name.

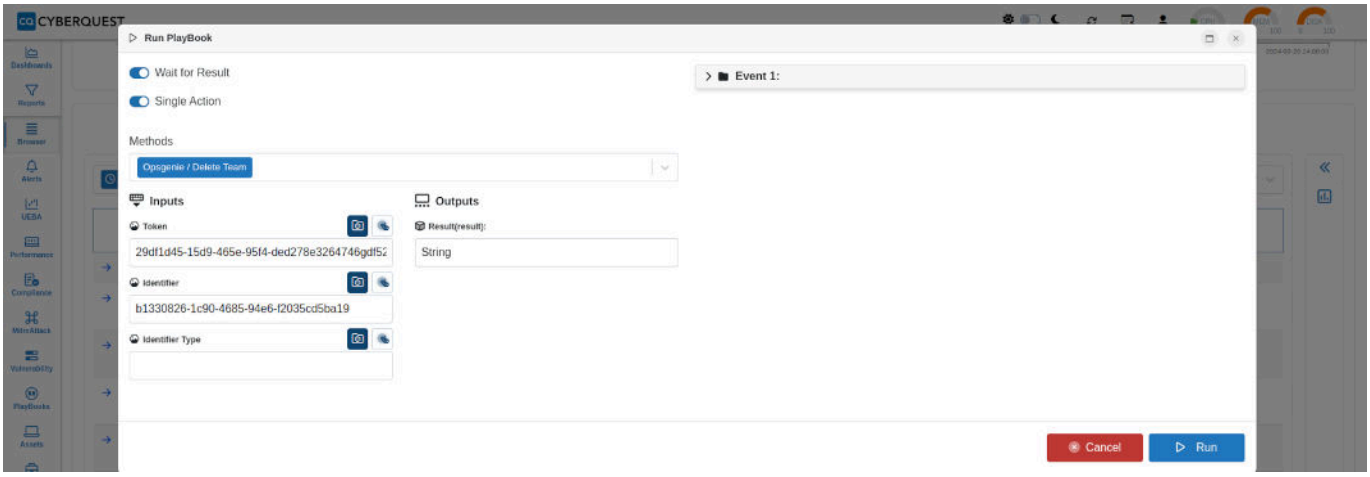


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Identifier (is required)	Identifier of the team
Identifier Type	Type of the identifier that is provided as an in-line parameter. Possible values are id and name. Default value is id

Outputs	Description
ID (data_id)	
Name (data_name)	
Description (data_description)	
Members (data_members)	

Opsgenie/Delete Team method

Returns team with given id or name.

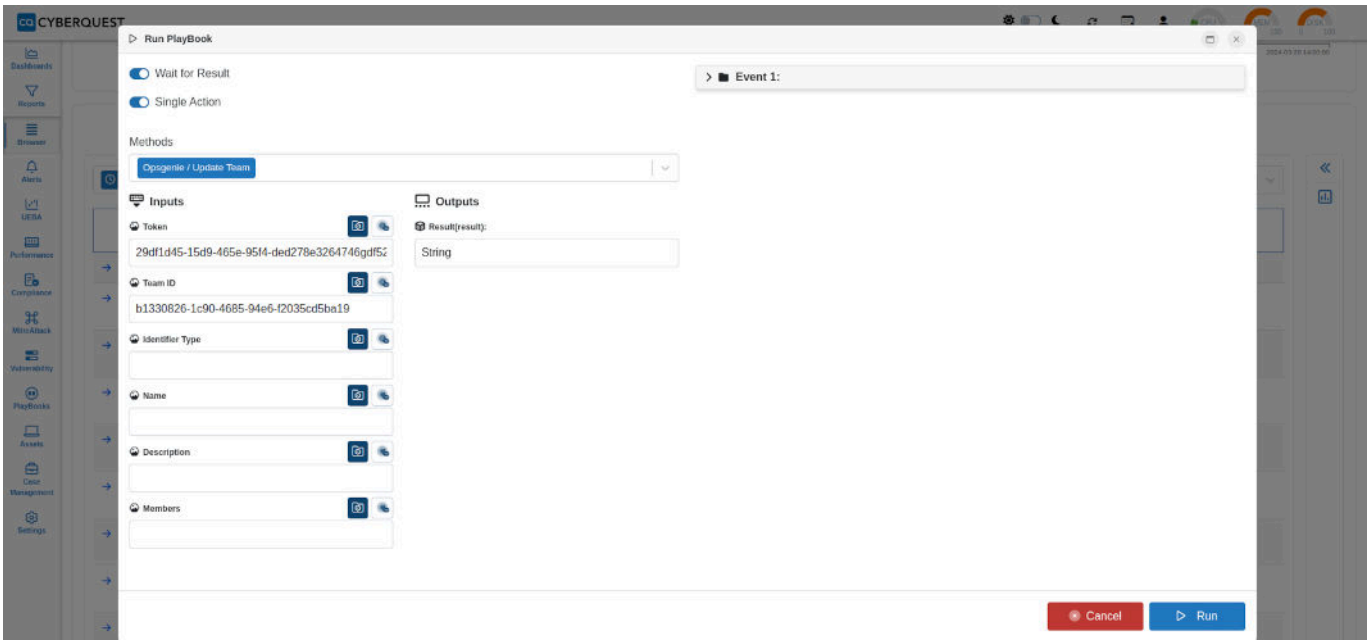


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Identifier (is required)	Identifier of the team
Identifier Type	Type of the identifier that is provided as an in-line parameter. Possible values are id and name. Default value is id

Outputs	Description
Result (result)	The result of the API call

Opsgenie/Update Team method

Update team with given id.

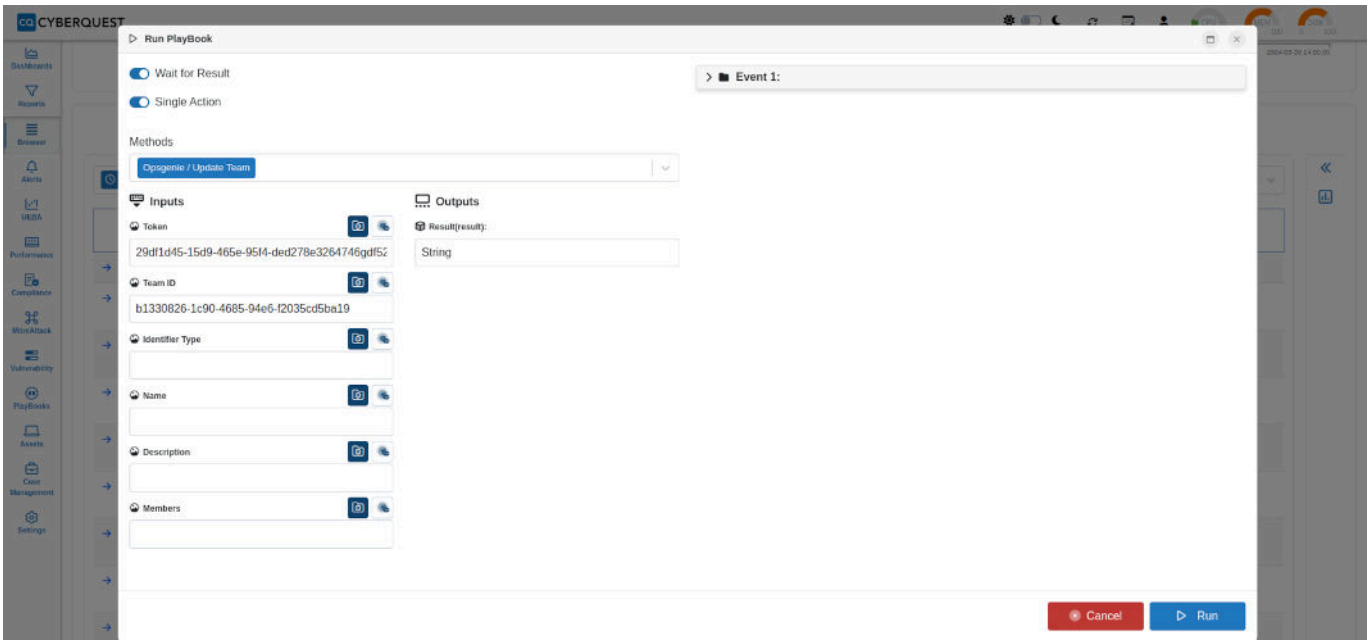


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Team ID (is required)	Identifier of the team
Identifier Type	Type of the identifier that is provided as an in-line parameter. Possible values are id and name. Default value is id
Name	The name of team
Description	The description of team
Members	The users which will be added to team, and optionally their roles.

Outputs	Description
Result (result)	The result of the API call

Opsgenie/List Team Logs method

Update team with given id.

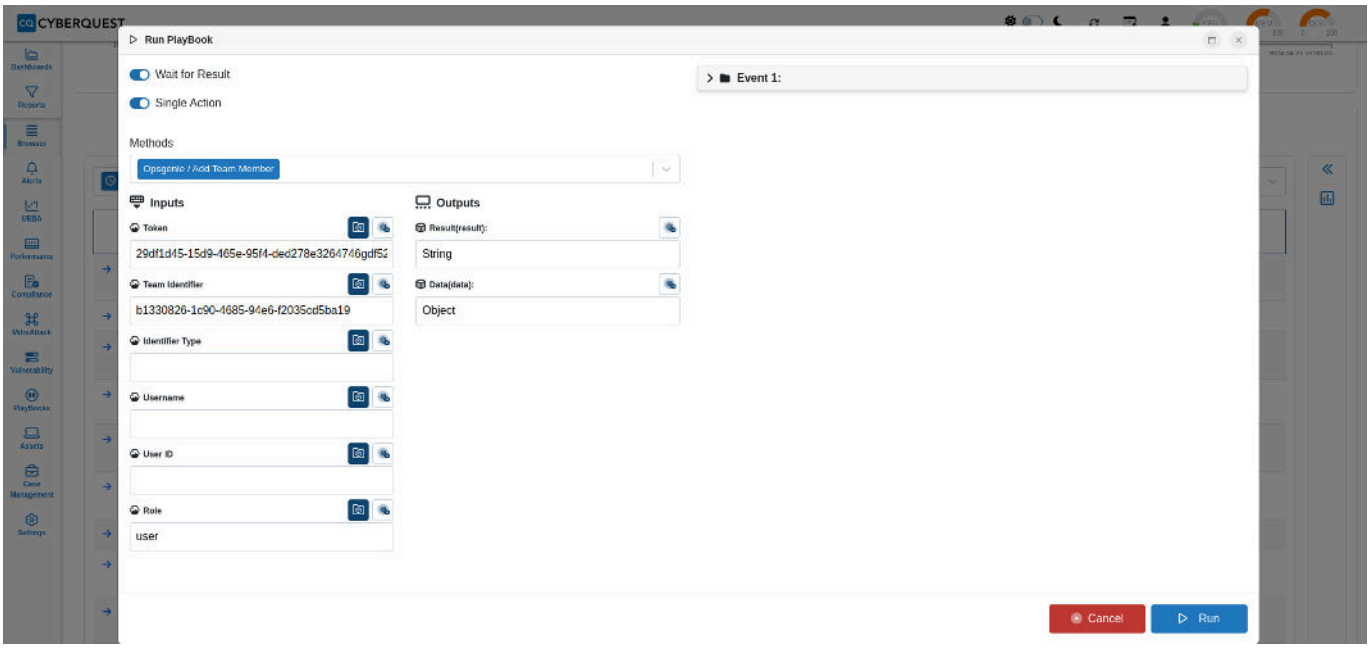


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key
Identifier (is required)	Identifier of the team
Identifier Type	Type of the identifier that is provided as an in-line parameter. Possible values are id and name. Default value is id
Limit	Maximum number of items to provide in the result. Must be a positive integer value. Default value is 20 and maximum is 100
Order	Sorting order of the result set. Possible values are desc and asc. Default value is desc
Offset	Key which will be used in pagination

Outputs	Description
Logs (data_logs)	The results of the API call

Opsgenie/Add Team Member method

Adds a member to team with given identifier.

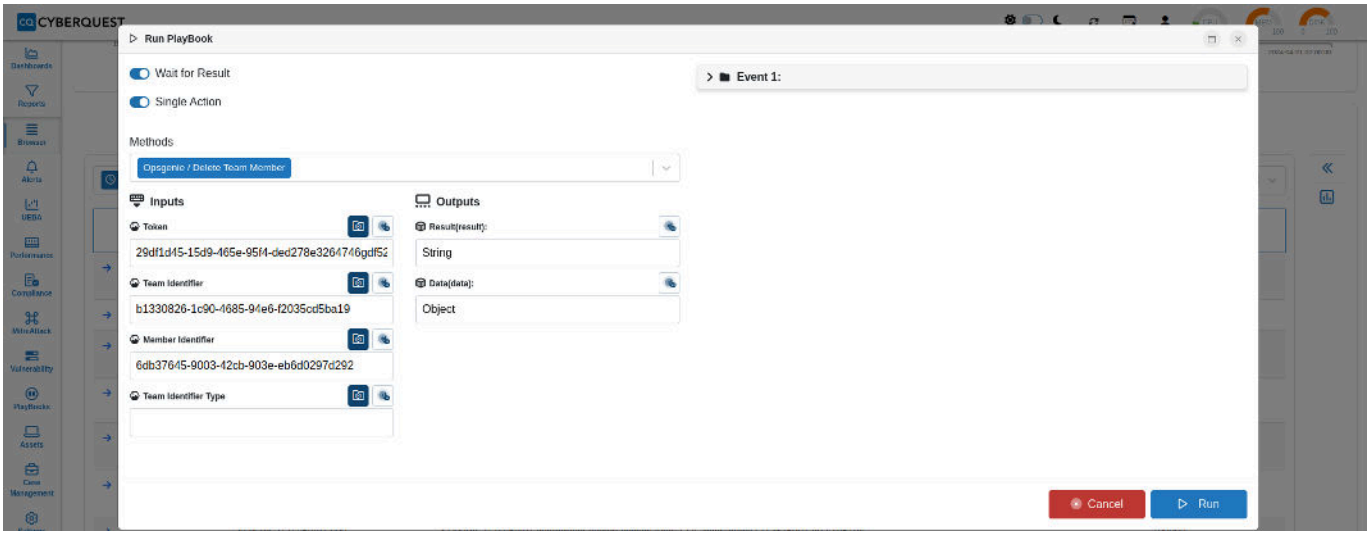


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Team Identifier (is required)	Identifier of the team
Identifier Type	Type of the identifier that is provided as an in-line parameter. Possible values are id and name. Default value is id
Username	Member identifier of the team, consisting id and/or username. Username or ID required!
User ID	Member identifier of the team, consisting id and/or username.Username or ID required!
Role	Member role of the user, consisting user and admin. Default value is user

Outputs	Description
Result (result)	The result of the API call
Data (data)	Details about the new team member

Opsgenie/Delete Team Member method

Remove team member.

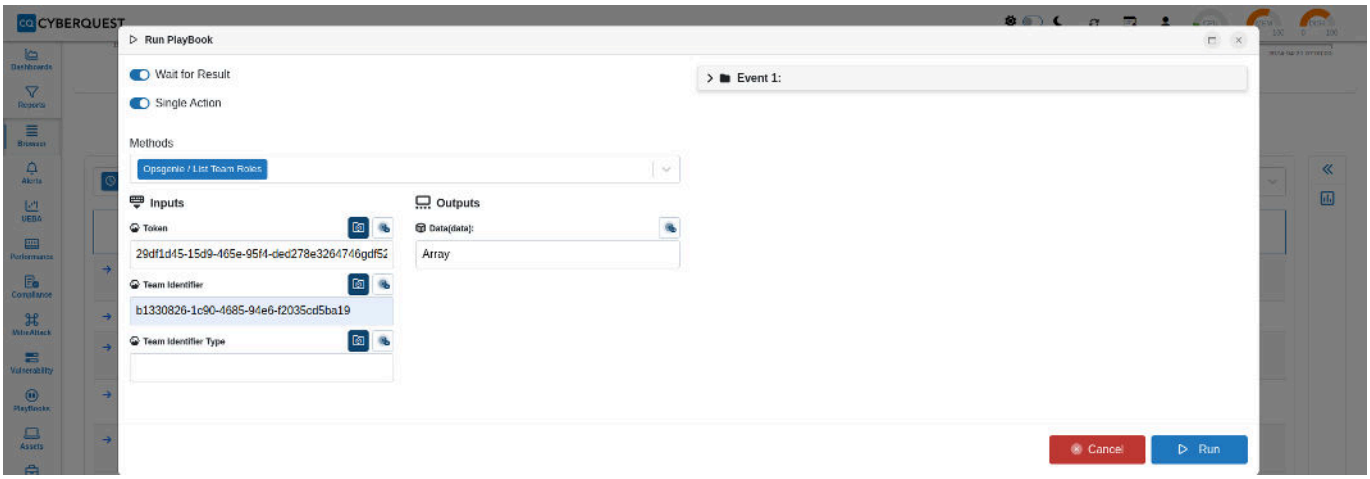


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Team Identifier (is required)	Identifier of the team
Member Identifier (is required)	User id or username of member for removal
Team Identifier Type	Type of the team identifier that is provided as an in-line parameter. Possible values are id and name . Default value is id

Outputs	Description
Result (result)	The result of the API call
Data (data)	Details about deleted team member

Opsgenie/List Team Roles method

Remove team member.

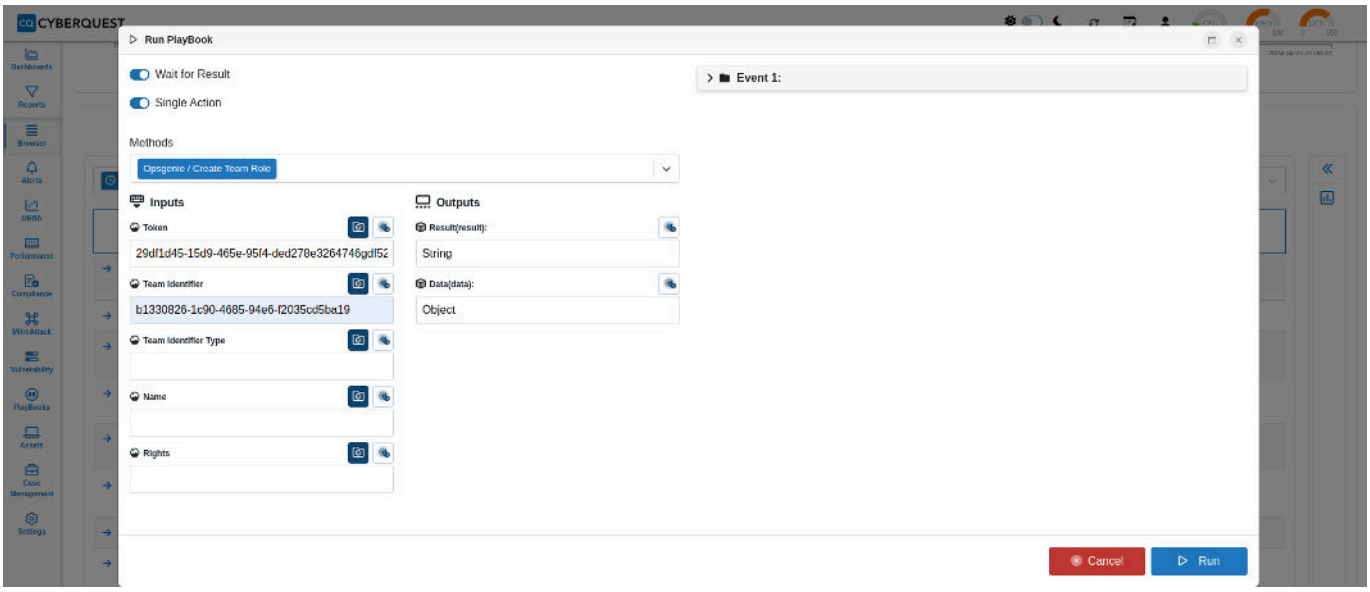


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Team Identifier (is required)	Identifier of the team
Team Identifier Type	Type of the team identifier that is provided as an in-line parameter. Possible values are id and name . Default value is id

Outputs	Description
Data (data)	The results of the API call

Opsgenie/Create Team Role method

Create team role.

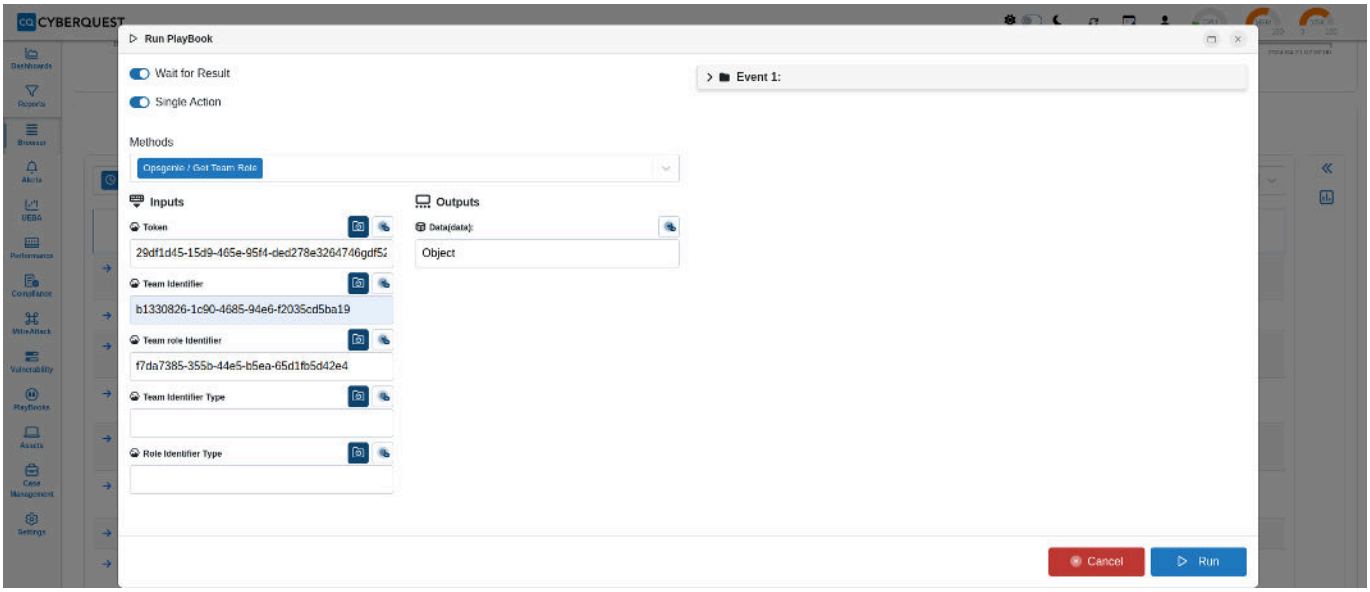


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Team Identifier (is required)	Identifier of the team
Team Identifier Type	Type of the team identifier that is provided as an in-line parameter. Possible values are id and name . Default value is id
Name	Name of the defined team role
Rights	You can refer Team Right for detailed information about team right and its fields

Outputs	Description
Result (result)	The result of the API call
Data (data)	Details about the new created team role

Opsgenie/Get Team Role method

Returns team role with given id or name.

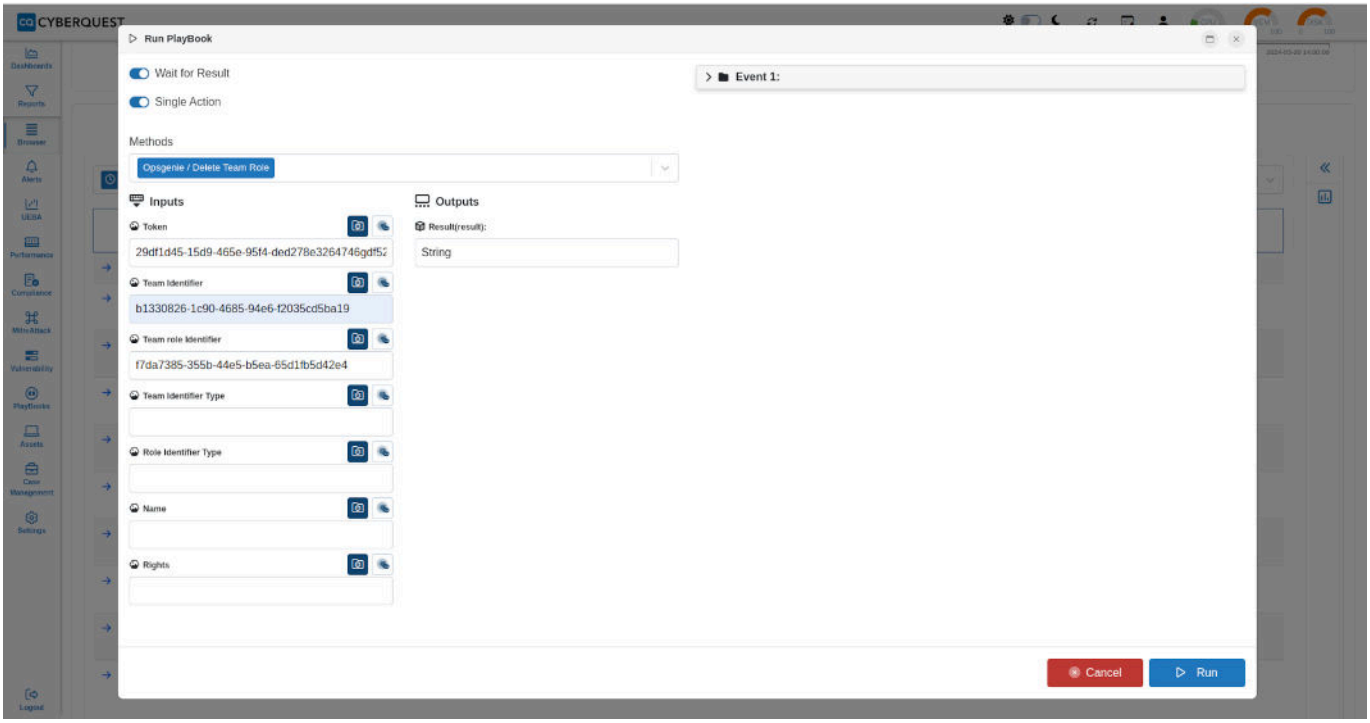


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Team Identifier (is required)	Identifier of the team
Team role Identifier (is required)	Identifier of the team role
Team Identifier Type	Type of the team identifier that is provided as an in-line parameter. Possible values are id and name . Default value is id
Role Identifier Type	Type of the team role identifier that is provided as an in-line parameter. Possible values are id and name . Default value is id

Outputs	Description
Data (data)	Details about team Role

Opsgenie/Delete Team Role method

Deletes a team role using team role id or name.

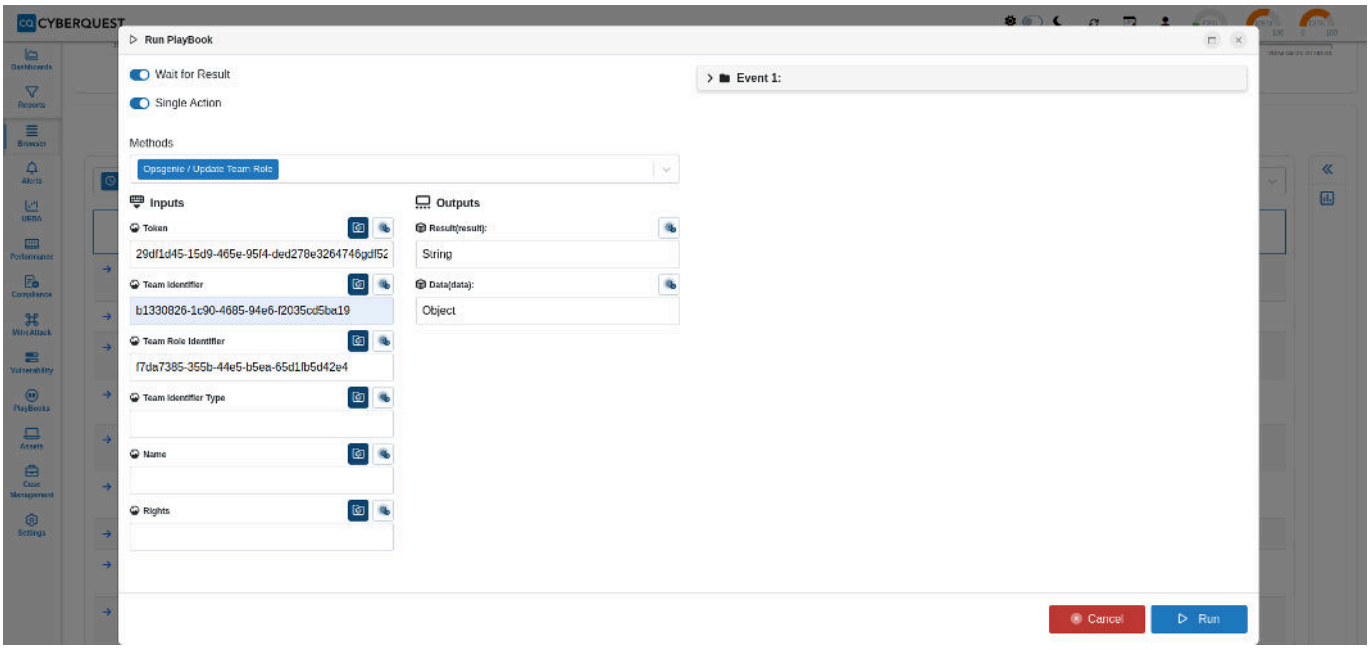


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Team Identifier (is required)	Identifier of the team
Team role Identifier (is required)	Identifier of the team role
Team Identifier Type	Type of the team identifier that is provided as an in-line parameter. Possible values are id and name . Default value is id
Role Identifier Type	Type of the team role identifier that is provided as an in-line parameter. Possible values are id and name . Default value is id
Name	Name of the team role
Rights	Type of the team role identifier that is provided as an in-line parameter. Possible values are id and name . Default value is id

Outputs	Description
Result (result)	The result of the API call

Opsgenie/Update Team Role method

Update team role.

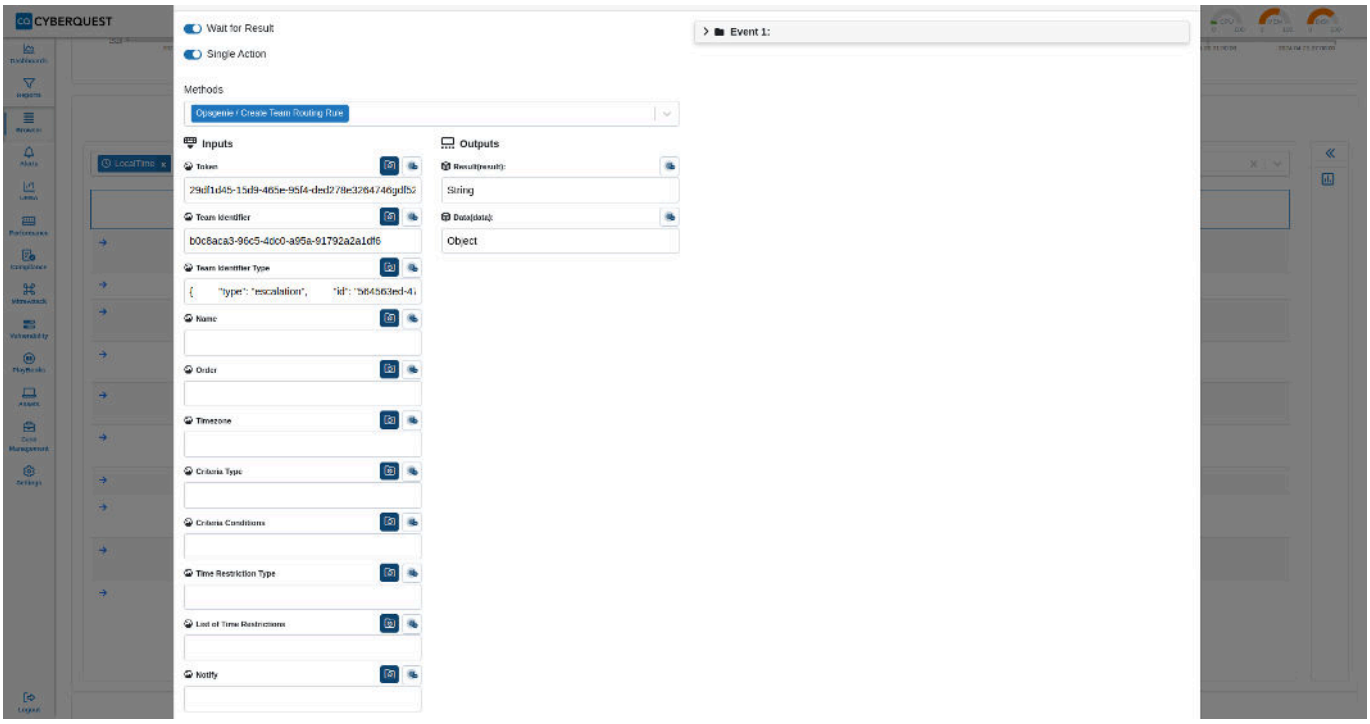


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Team Identifier (is required)	Identifier of the team
Team Role Identifier (is required)	Identifier of the team role
Team Identifier Type	Type of the team identifier that is provided as an in-line parameter. Possible values are id and name . Default value is id
Name	Name of the defined team role
Rights	You can refer Team Right for detailed information about team right and its fields

Outputs	Description
Result (result)	The result of the API call
Data (data)	Details about the updated team role

Opsgenie/Create Team Routing Rule method

Returns team role with given id or name.

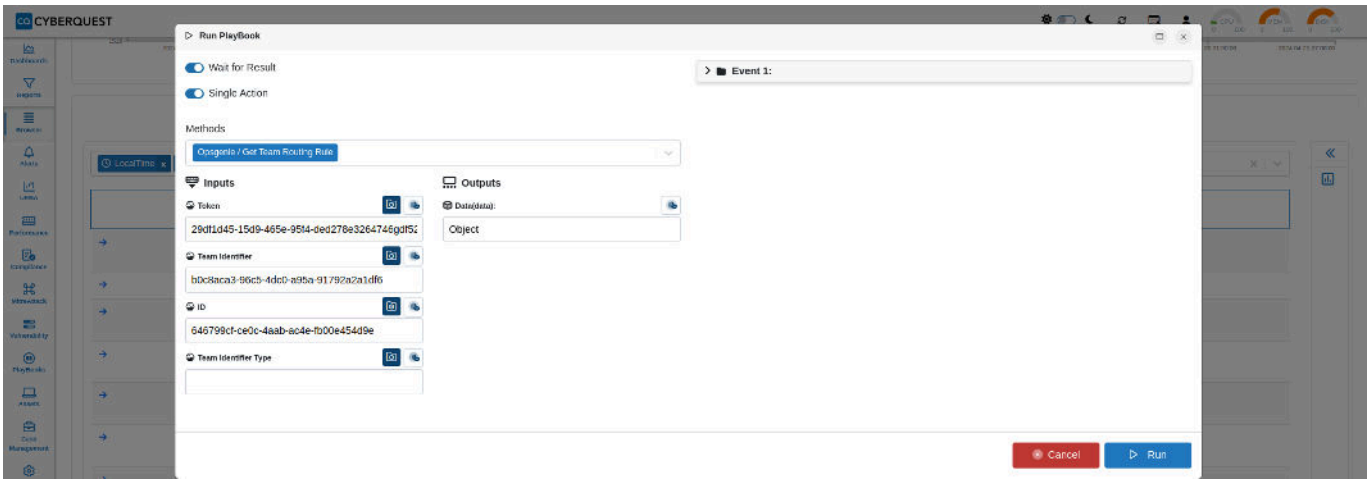


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Team Identifier (is required)	Identifier of the team
Team Identifier Type	Type of the team identifier that is provided as an in-line parameter. Possible values are id and name . Default value is id
Name	Name of the team routing rule
Order	The order of the team routing rule within the rules. order value is actually the index of the team routing rule whose minimum value is 0 and whose maximum value is n-1 (number of team routing rules is n)
Timezone	Timezone of team routing rule. If timezone field is not given, account timezone is used as default.
Criteria Type	Defines the conditions that will be checked before applying team routing rule and type of the operations that will be applied on these conditions
Criteria Conditions	Defines the conditions that will be checked before applying team routing rule and type of the operations that will be applied on these conditions
Time Restriction Type	This parameter should be set time-of-day
List of Time Restrictions	It is a restriction object which is described: startHour = Value of the hour that team routing rule start workingstartMin = Value of the minute that team routing rule start workingendHour = Value of the hour that team routing rule end workingendMin = Value of the minute that team routing rule end working
Notify	Target entity of schedule, escalation, or the reserved word none which will be notified in routing rule. The possible values for notify type are:scheduleescalation* none

Outputs	Description
Result (result)	The result of the API call
Data (data)	Details about team routing rule

Opsgenie/Get Team Routing Rule method

Returns team routing rule with given id.

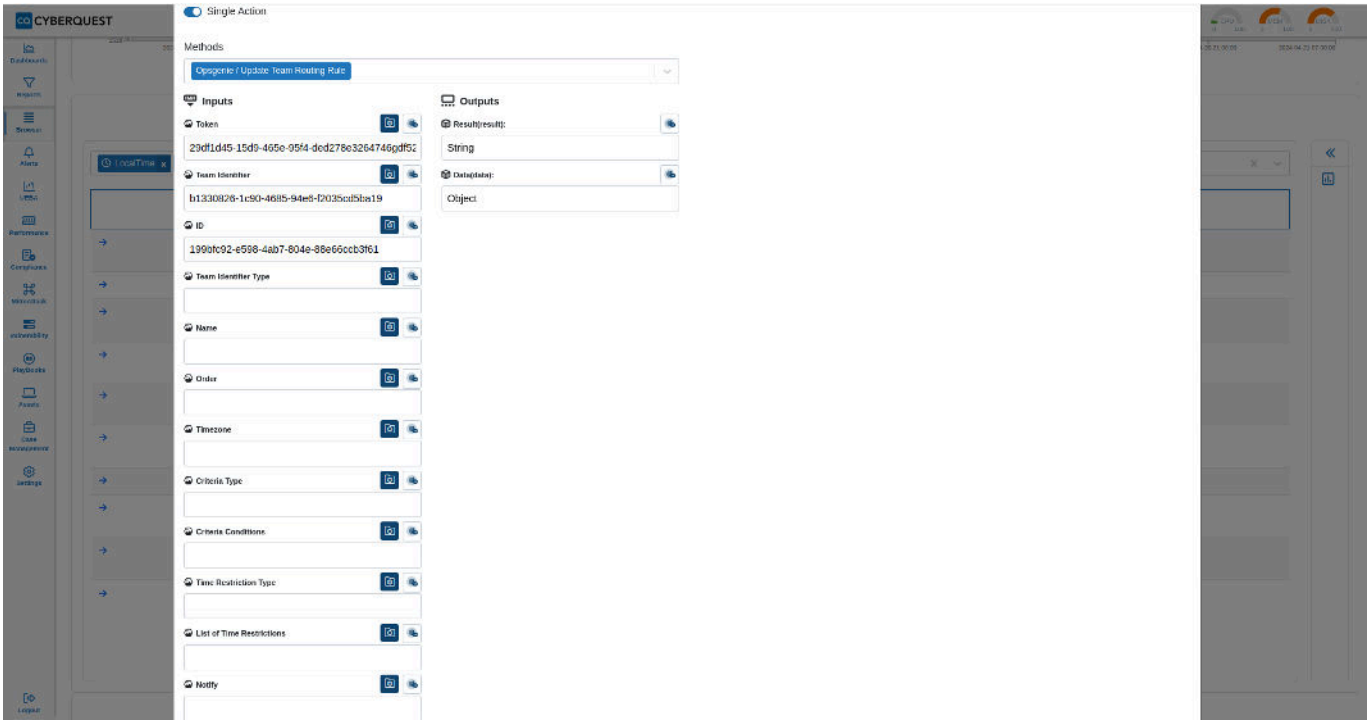


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Team Identifier (is required)	Identifier of the team
ID (is required)	Id of the team routing rule
Team Identifier Type	Type of the team identifier that is provided as an in-line parameter. Possible values are id and name . Default value is id

Outputs	Description
Data (data)	Details about team routing rule

Opsgenie/Update Team Routing Rule method

Update routing rule of the team.

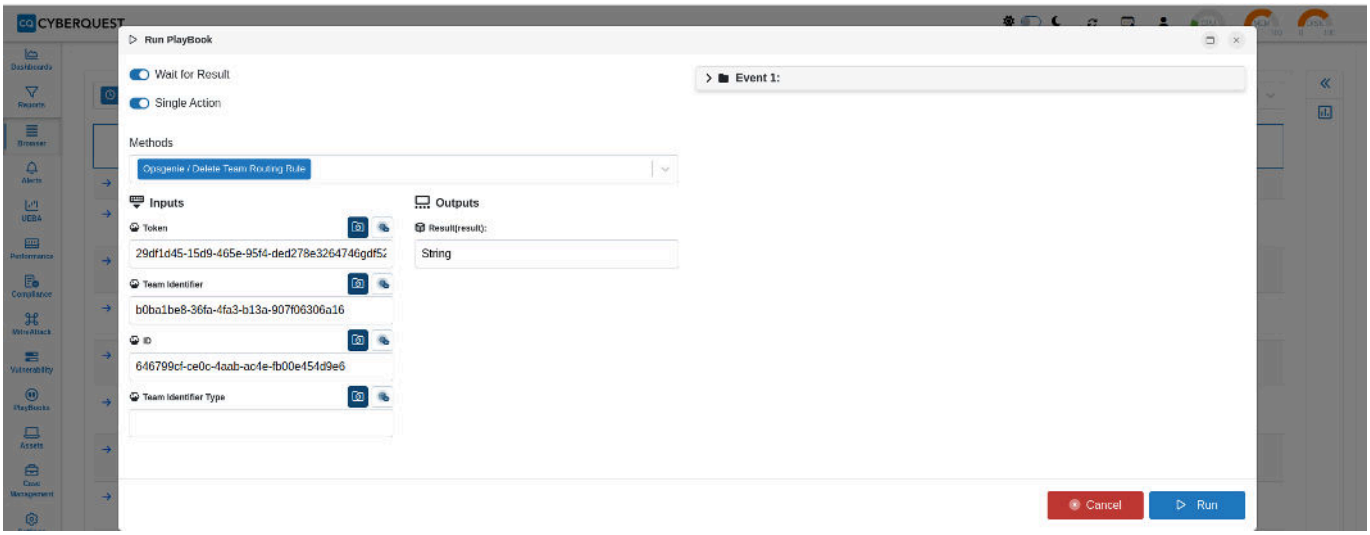


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Team Identifier (is required)	Identifier of the team
ID (is required)	Id of the team routing rule
Team Identifier Type	Type of the team identifier that is provided as an in-line parameter. Possible values are id and name . Default value is id
Name	Name of the team routing rule
Order	The order of the team routing rule within the rules. order value is actually the index of the team routing rule whose minimum value is 0 and whose maximum value is n-1 (number of team routing rules is n)
Timezone	Timezone of team routing rule. If timezone field is not given, account timezone is used as default.
Criteria Type	Defines the conditions that will be checked before applying team routing rule and type of the operations that will be applied on these conditions
Criteria Conditions	Defines the conditions that will be checked before applying team routing rule and type of the operations that will be applied on these conditions
Time Restriction Type	This parameter should be set time-of-day
List of Time Restrictions	It is a restriction object which is described: startHour = Value of the hour that team routing rule start workingstartMin = Value of the minute that team routing rule start workingendHour = Value of the hour that team routing rule end workingendMin = Value of the minute that team routing rule end working
Notify	Target entity of schedule, escalation, or the reserved word none which will be notified in routing rule. The possible values for notify type are:scheduleescalation* none

Outputs	Description
Result (result)	The result of the API call
Data (data)	Details about updated team routing rule

Opsgenie/Delete Team Routing Rule method

Delete team routing rule with given id.

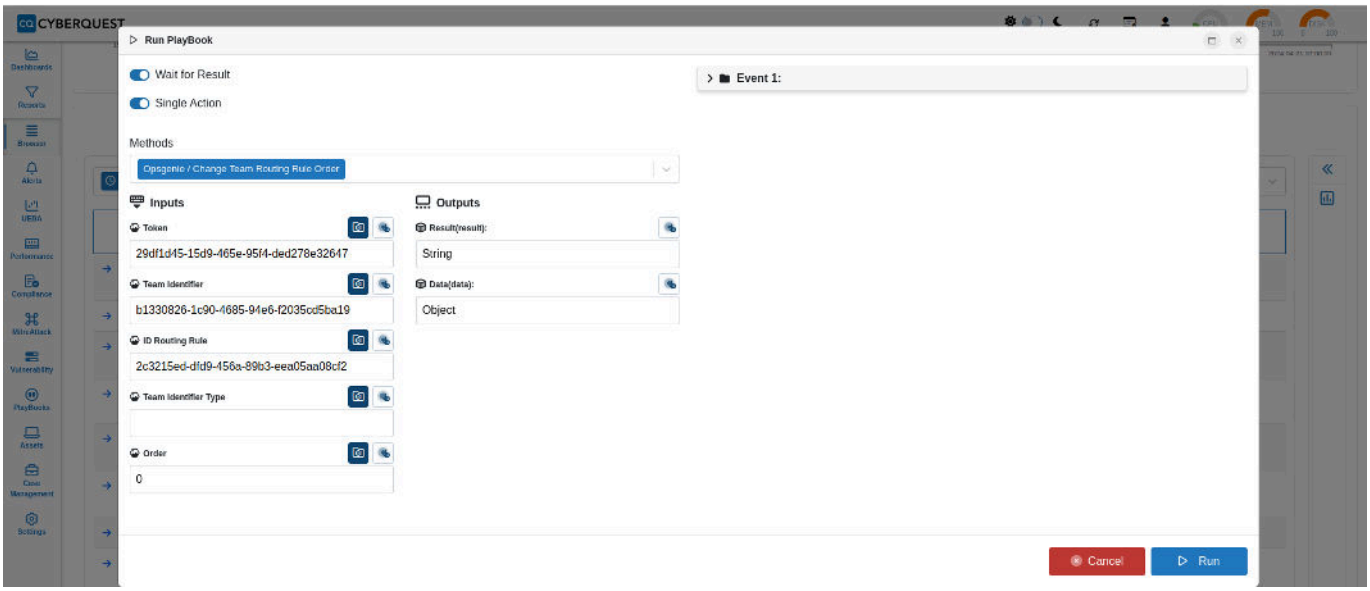


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Team Identifier (is required)	Identifier of the team
ID (is required)	Id of the team routing rule
Team Identifier Type	Type of the team identifier that is provided as an in-line parameter. Possible values are id and name . Default value is id

Outputs	Description
Result (result)	The result of the API call

Opsgenie/Change Team Routing Rule Order method

Change the order of team routing rule with given id.

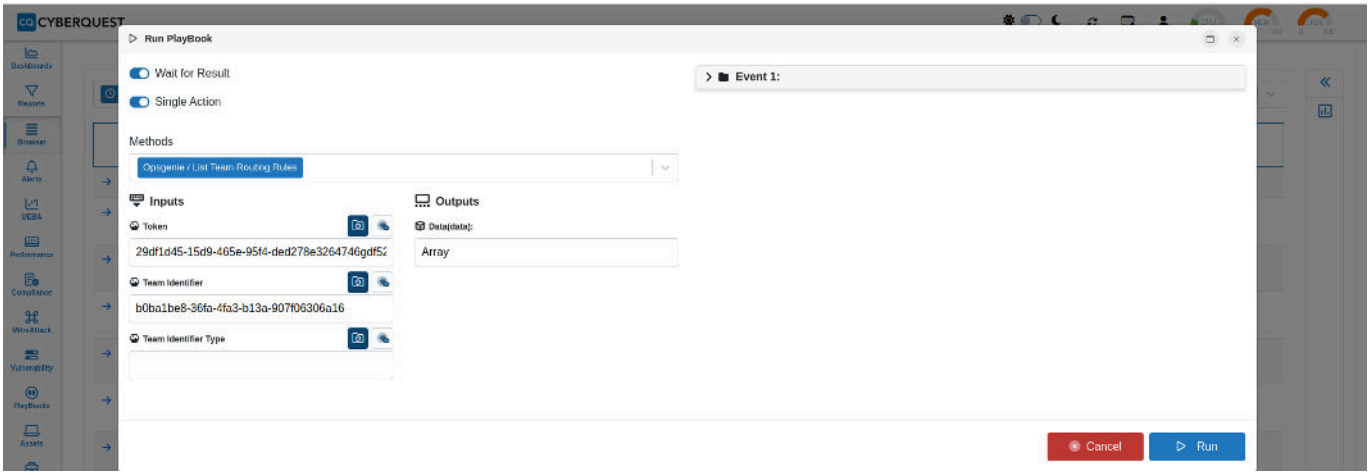


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Team Identifier (is required)	Identifier of the team
ID Routing Rule (is required)	Id of the team routing rule
Team Identifier Type	Type of the team identifier that is provided as an in-line parameter. Possible values are id and name . Default value is id
Order (is required)	The order of the team routing rule within the rules. Value is actually the index of the team routing rule whose minimum value is 0 and whose maximum value is n-1 (number of team routing rules is n).

Outputs	Description
Result (result)	The result of the API call
Data (data)	Details about the changed order team routing rule

Opsgenie/List Team Routing Rules method

Returns list of team routing rules.

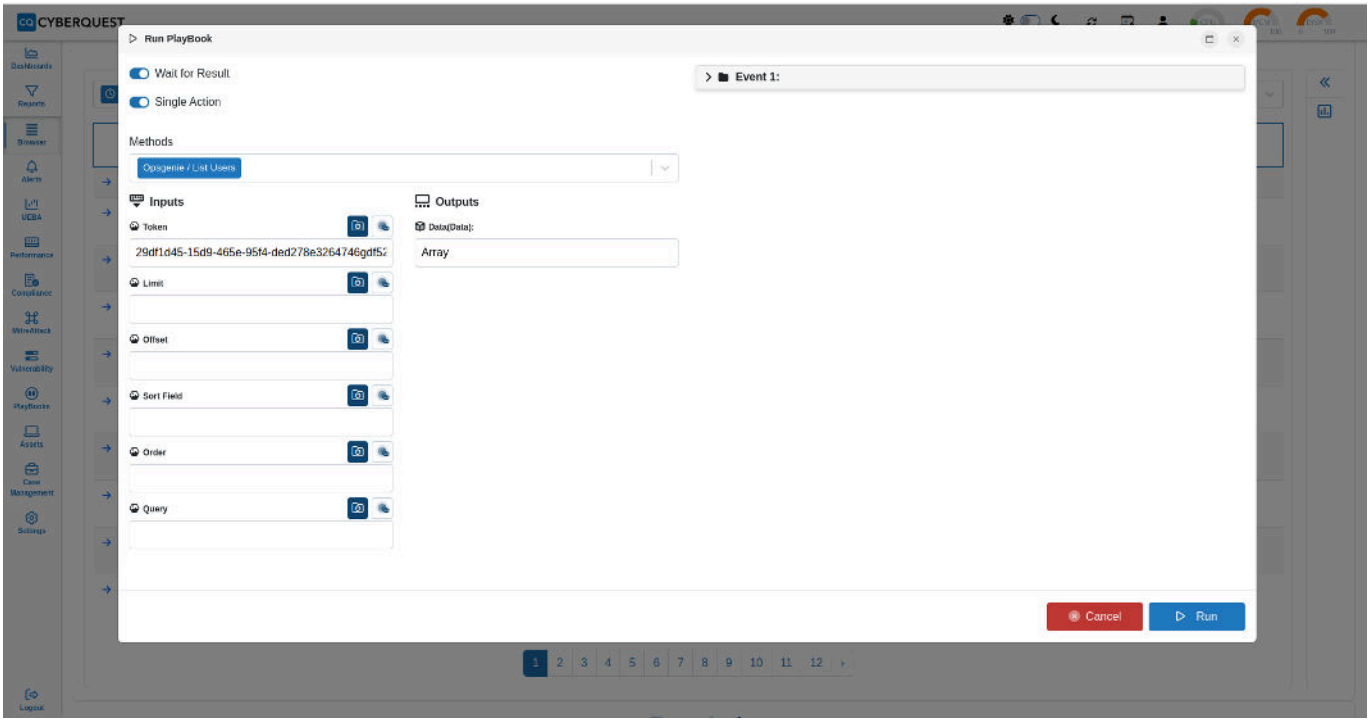


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Team Identifier (is required)	Identifier of the team
Team Identifier Type	Type of the team identifier that is provided as an in-line parameter. Possible values are id and name . Default value is id

Outputs	Description
Data (data)	The results of the API call

Opsgenie/List Users method

List users with given parameters.

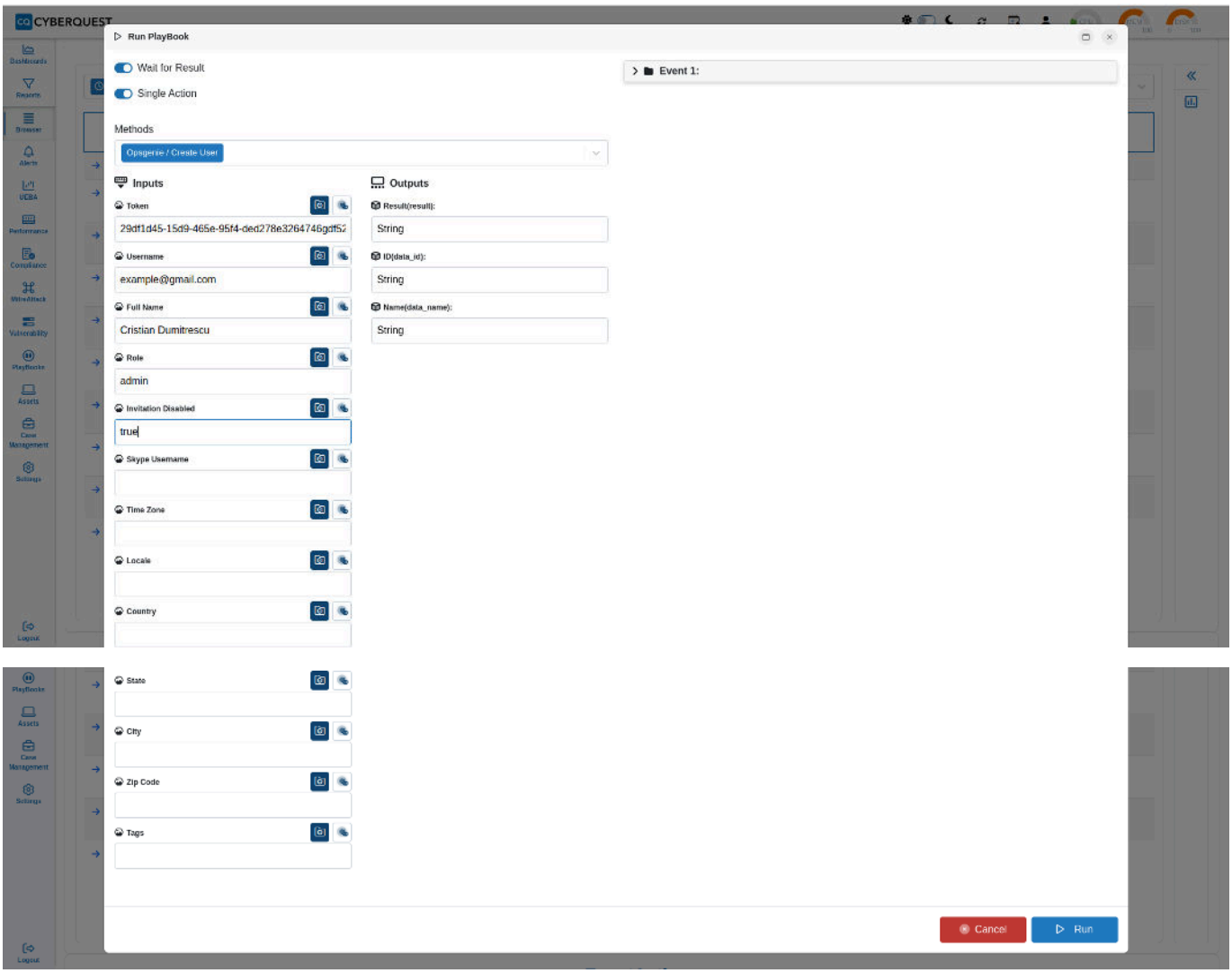


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Limit	Number of users to retrieve
Offset	Number of users to skip from start
Sort Field	Field to use in sorting. Should be one of username, fullName and insertedAt
Order	Direction of sorting. Should be one of asc or desc
Query	Field:value combinations with most of user fields to make more advanced searches. Possible fields are username, fullName, blocked, verified, role, locale, timeZone, userAddress and createdAt

Outputs	Description
Data (Data)	The results of the API call

Opsgenie/Create User method

Creates a user with the given payload.

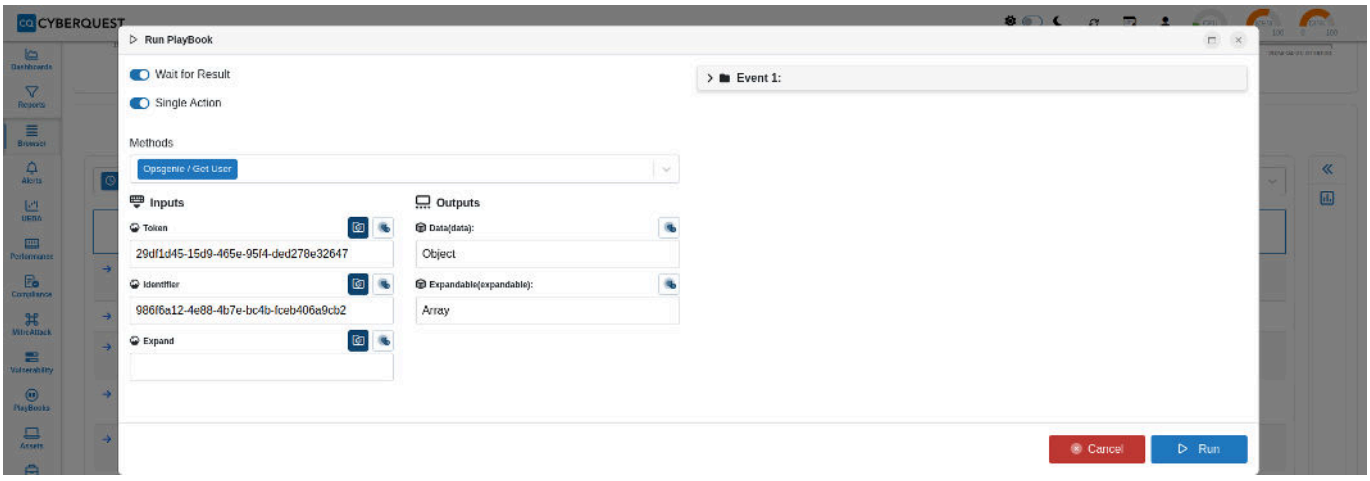


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Username (is required)	E-mail address of the user
Full Name (is required)	Name of the user
Role (is required)	Role of user. It may be one of admin, user or the name of a custom role you haeve created.
Invitation Disabled	Invitation email will not be sent if set to true. Default value is false
Skype Username	Skype username of the user
Time Zone	Timezone of the user. If not set, timezone of the customer will be used instead.
Locale	Location information of the user. If not set, locale of the customer will be used instead.
Country	User Country
State	User State
City	User City
Zip Code	User Zip Code
Tags	ist of labels attached to the user. You can label users to differentiate them from the rest. For example, you can add ITManager tag to differentiate people with this role from others.

Outputs	Description
Result (result)	The result of the API call
ID (data_id)	The ID of the new created user
Name (data_name)	The name of the user

Opsgenie/Get User method

Get user for the given identifier.

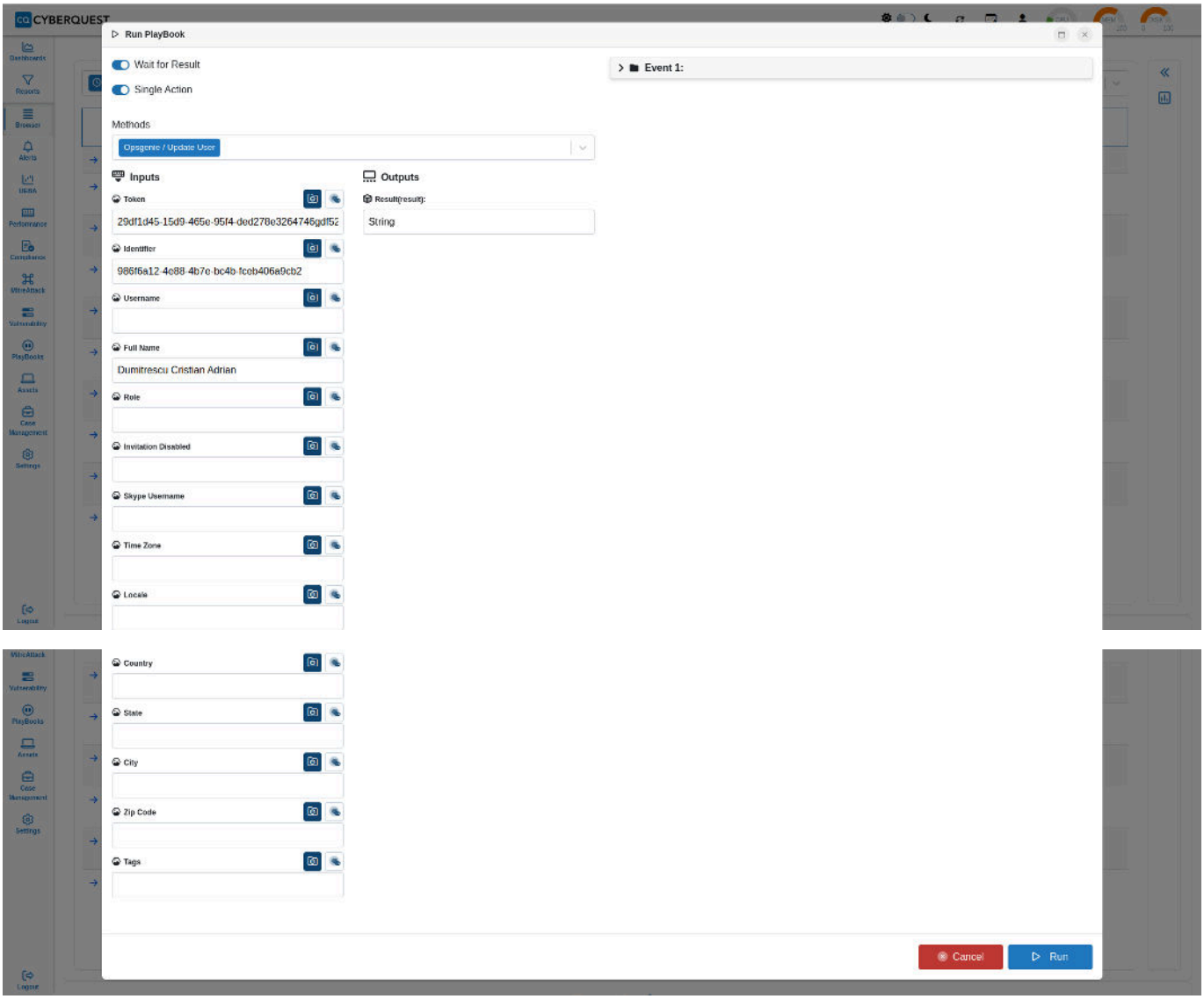


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Identifier (is required)	Identifier of the user to be searched
Expand	Comma separated list of strings to create a more detailed response. The only expandable field for user api is contact

Outputs	Description
Data (data)	Details about the user
Expandable (expandable)	A list with the additional details in the API response

Opsgenie/Update User method

Update user with the given identifier.

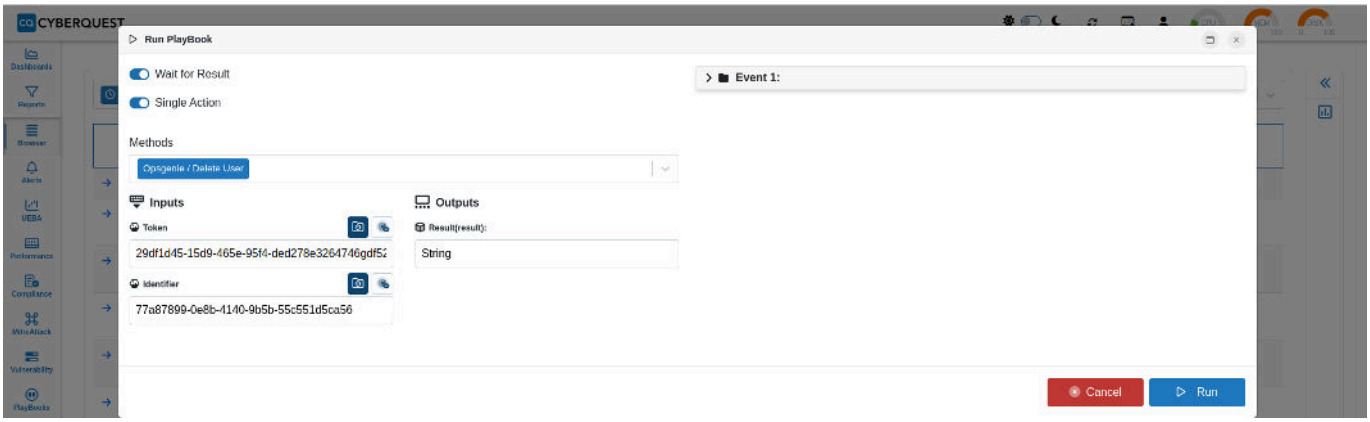


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Identifier (is required)	Identifier of the user to be searched
Username	E-mail address of the user
Full Name (is required)	Name of the user
Role	Role of user. It may be one of admin, user or the name of a custom role you have created.
Invitation Disabled	Invitation email will not be sent if set to true. Default value is false
Skype Username	Skype username of the user
Time Zone	Timezone of the user. If not set, timezone of the customer will be used instead.
Locale	Location information of the user. If not set, locale of the customer will be used instead.
Country	User Country
State	User State
City	User City
Zip Code	User Zip Code
Tags	ist of labels attached to the user. You can label users to differentiate them from the rest. For example, you can add ITManager tag to differentiate people with this role from others.

Outputs	Description
Result (result)	The result of the API call

Opsgenie/Delete User method

Delete user with the given identifier.

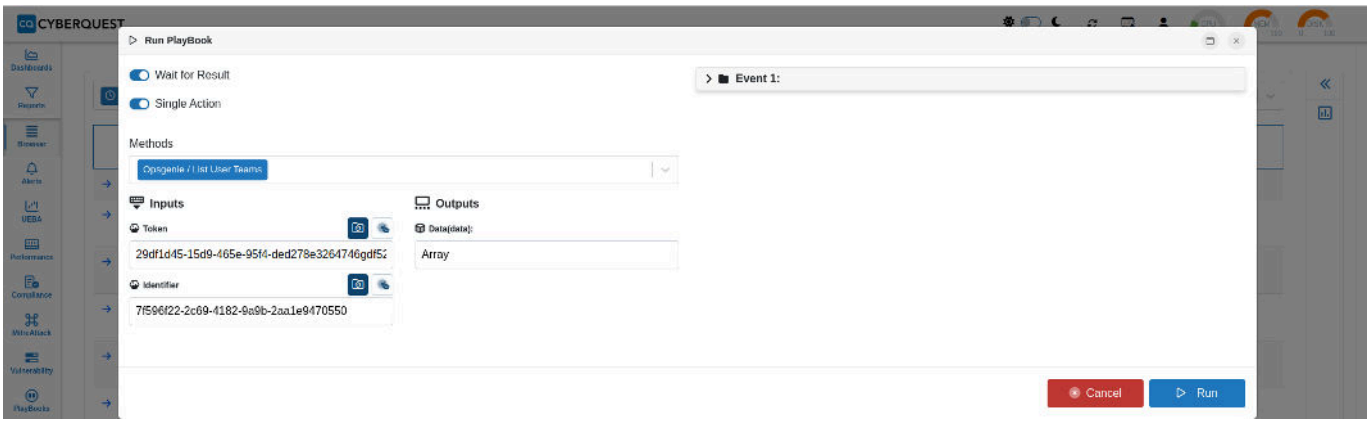


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Identifier (is required)	Identifier of the user to be searched

Outputs	Description
Result (result)	The result of the API call

Opsgenie/List User Teams method

List user teams for the given user identifier.

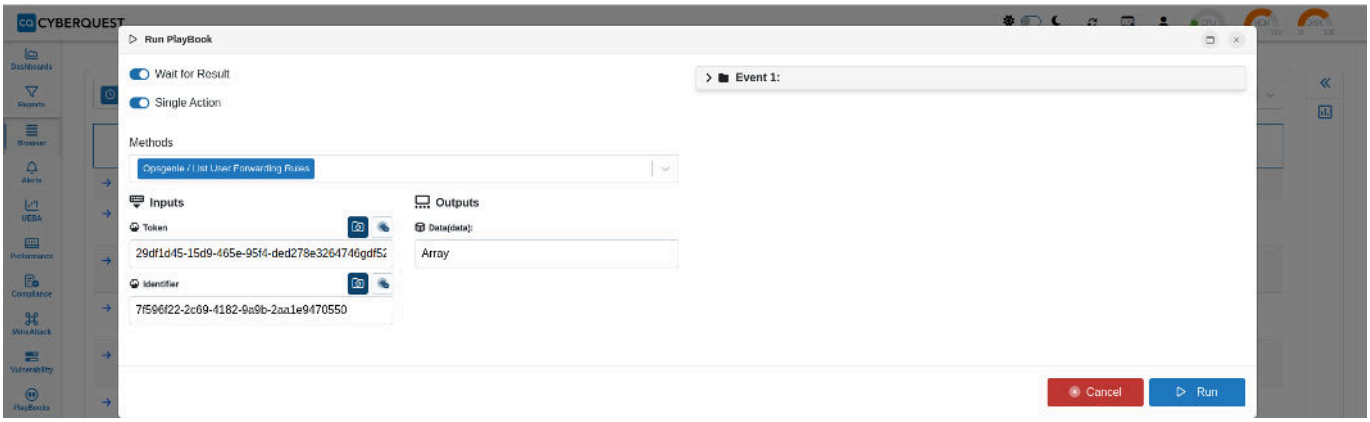


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Identifier (is required)	Identifier of the user to be searched

Outputs	Description
Data (data)	The results of the API call

Opsgenie/List User Forwarding Rules method

List user forwarding rules for the given user identifier.

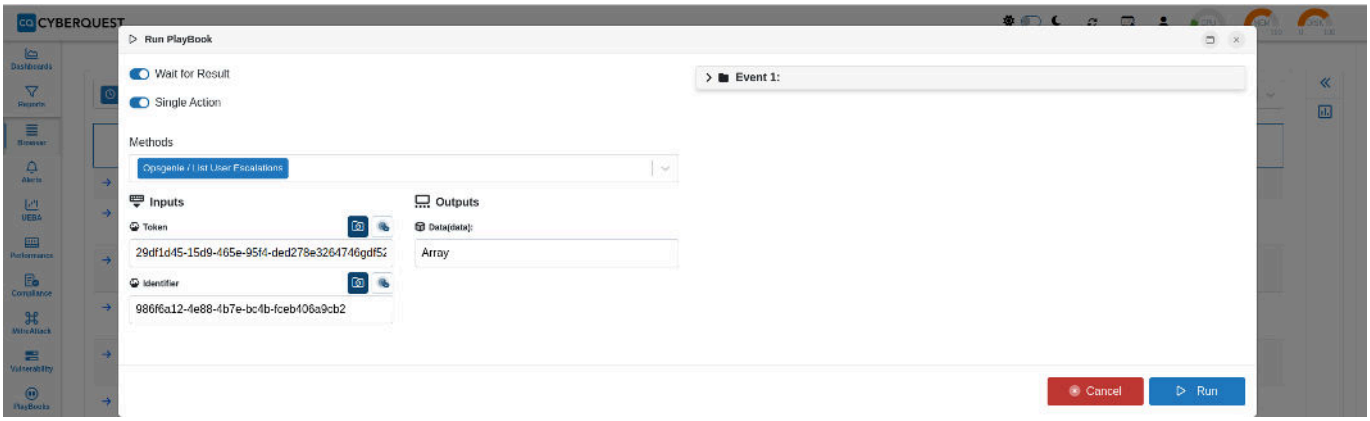


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Identifier (is required)	Identifier of the user to be searched

Outputs	Description
Data (data)	The results of the API call

Opsgenie/List User Escalations method

List escalations of the user for the given identifier.

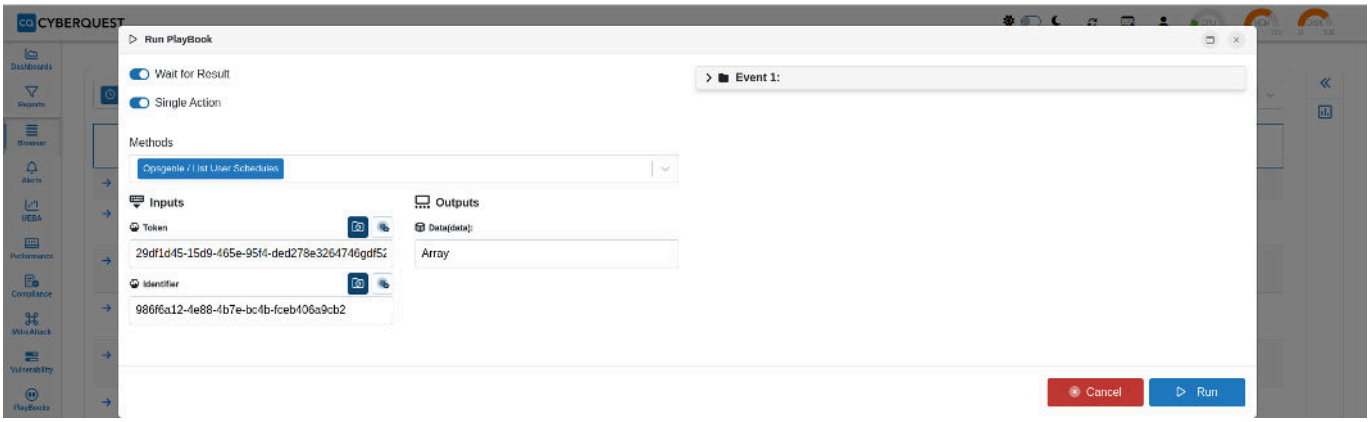


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Identifier (is required)	Identifier of the user to be searched

Outputs	Description
Data (data)	The results of the API call

Opsgenie/List User Schedules method

List schedules of the user for the given identifier.

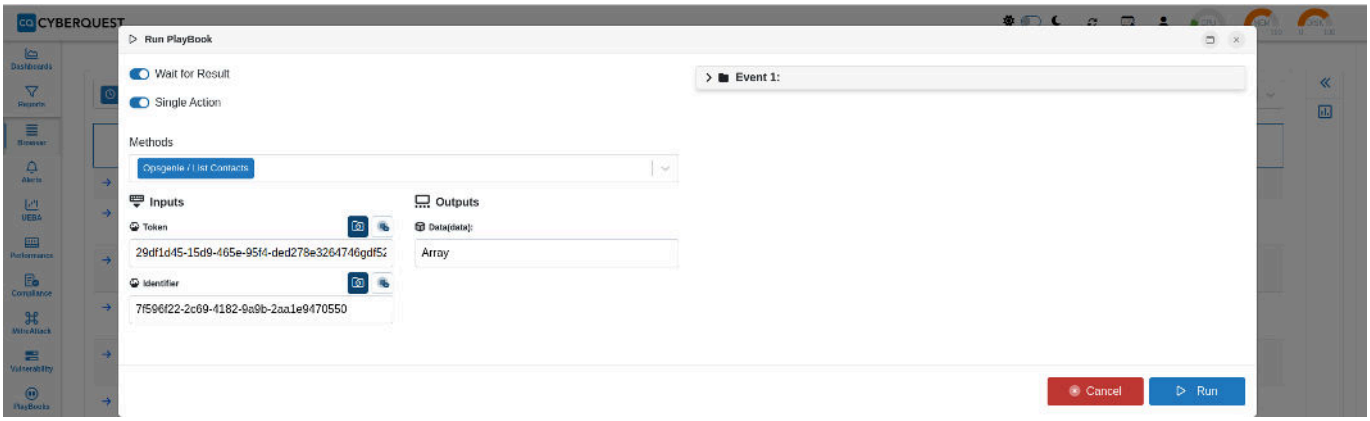


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Identifier (is required)	Identifier of the user to be searched

Outputs	Description
Data (data)	The results of the API call

Opsgenie/List Contacts method

Returns list of contacts.

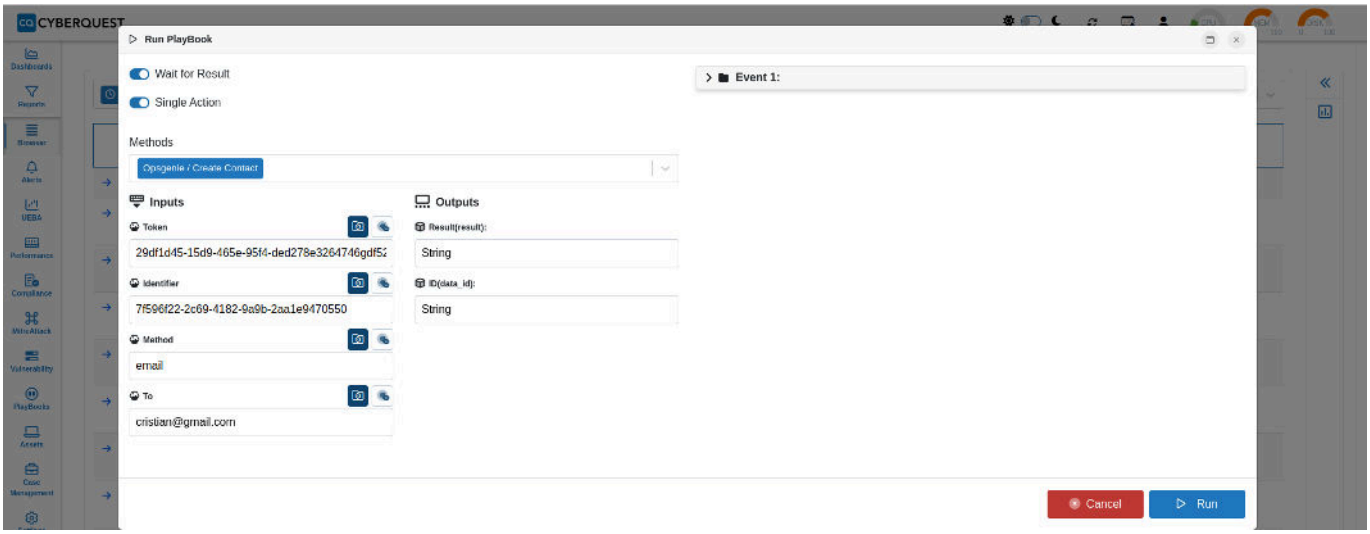


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Identifier (is required)	Identifier of the user to be searched

Outputs	Description
Data (data)	The results of the API call

Opsgenie/Create Contact method

Creates a new contact.

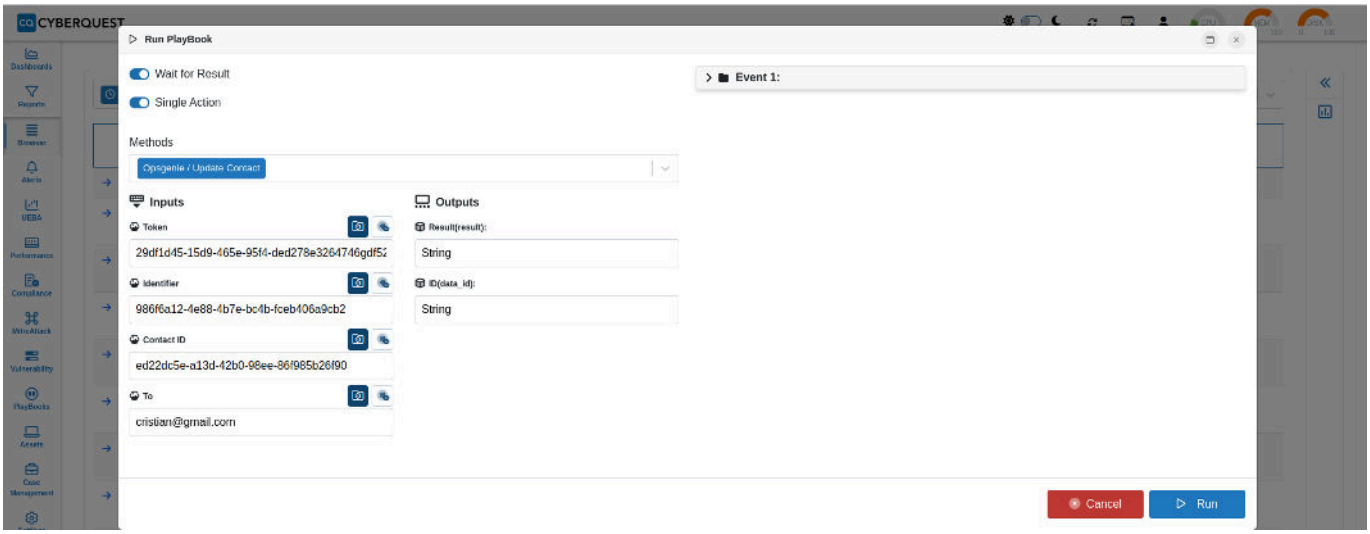


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Identifier (is required)	Identifier of the user to be searched
Method (is required)	Id of the contact
To (is required)	Address of contact method

Outputs	Description
Result (result)	The result of the API call
ID (data_id)	The ID of the created contact

Opsgenie/Update Contact method

Returns list of contacts.

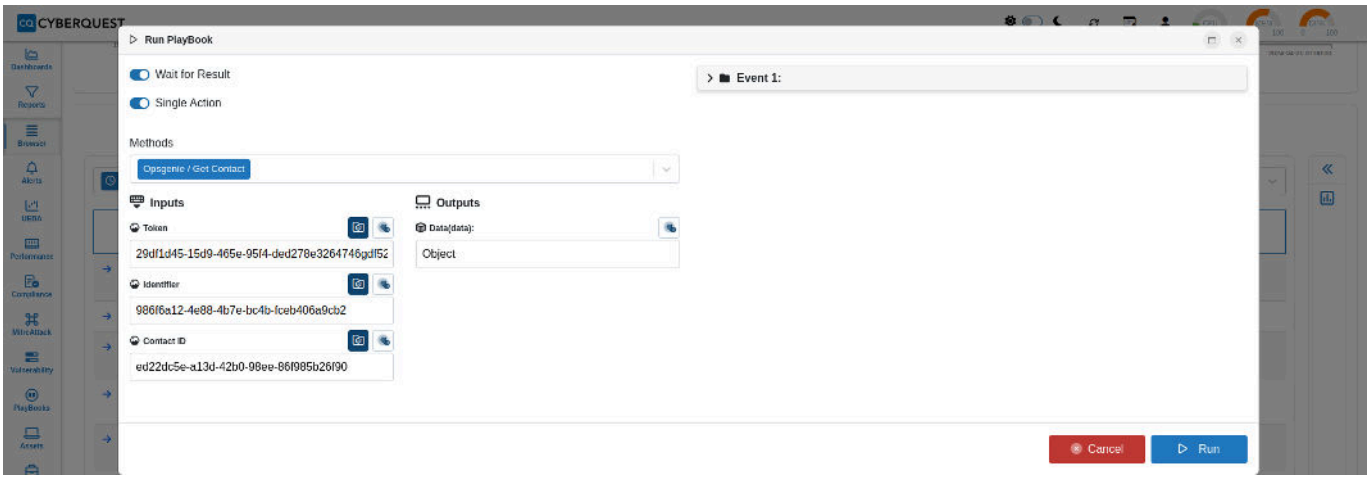


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Identifier (is required)	Identifier of the user to be searched
Contact ID (is required)	Id of the contact
To (is required)	Address of contact method

Outputs	Description
Result (result)	The result of the API call
ID (data_id)	The new contact ID

Opsgenie/Get Contact method

Returns contact with given id.

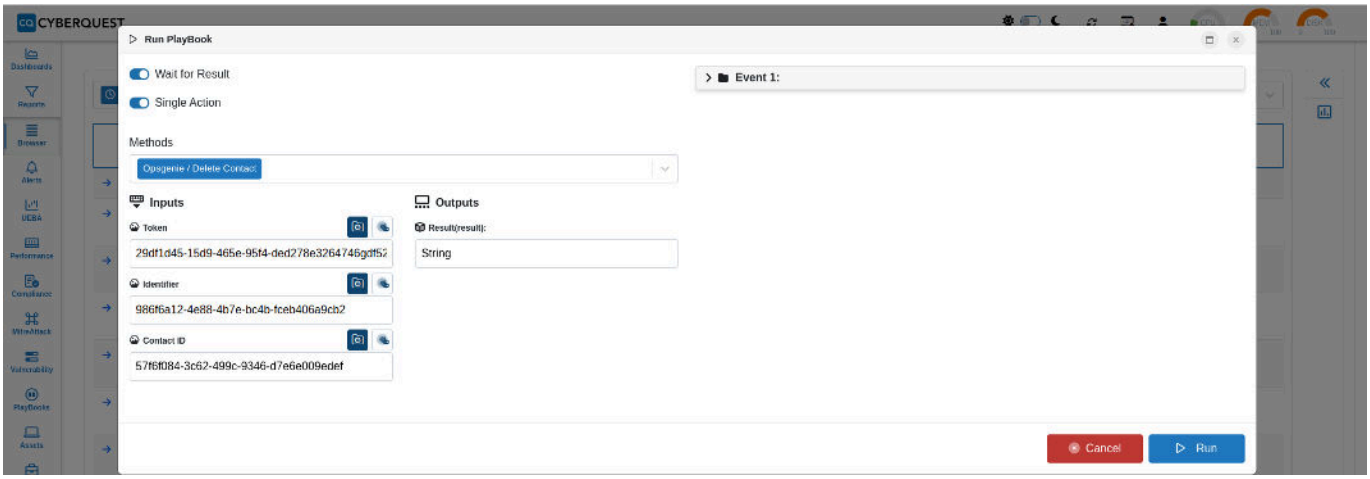


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Identifier (is required)	Identifier of the user to be searched
Contact ID (is required)	Id of the contact

Outputs	Description
Data (data)	The result of the API call

Opsgenie/Delete Contact method

Delete contact using contact id.

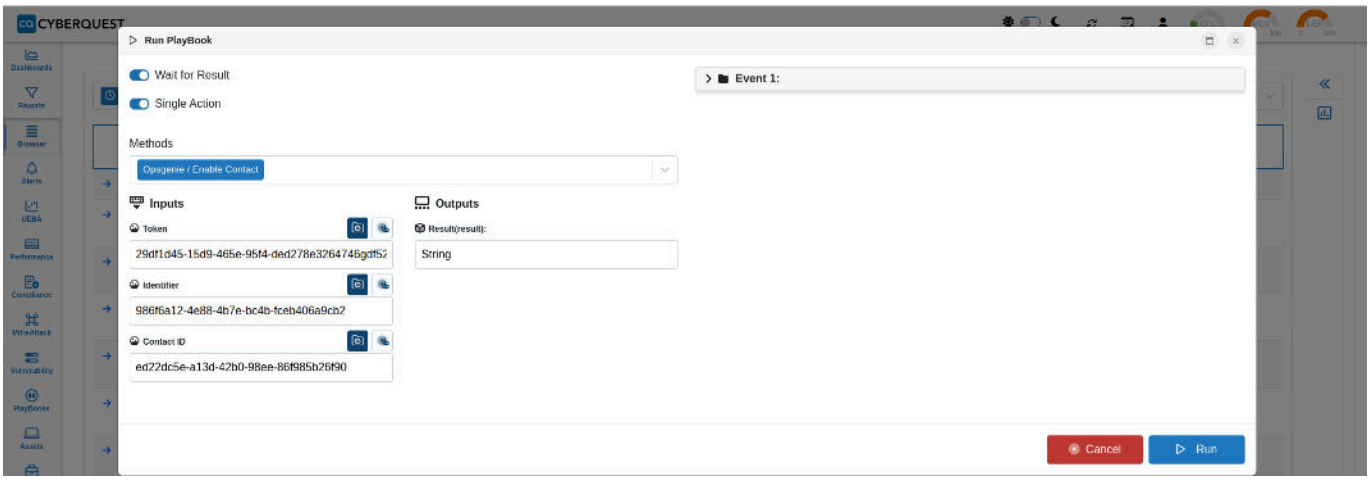


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Identifier (is required)	Identifier of the user to be searched
Contact ID (is required)	Id of the contact

Outputs	Description
Result (result)	The result of the API call

Opsgenie/Enable Contact method

Enable the contact of the user.

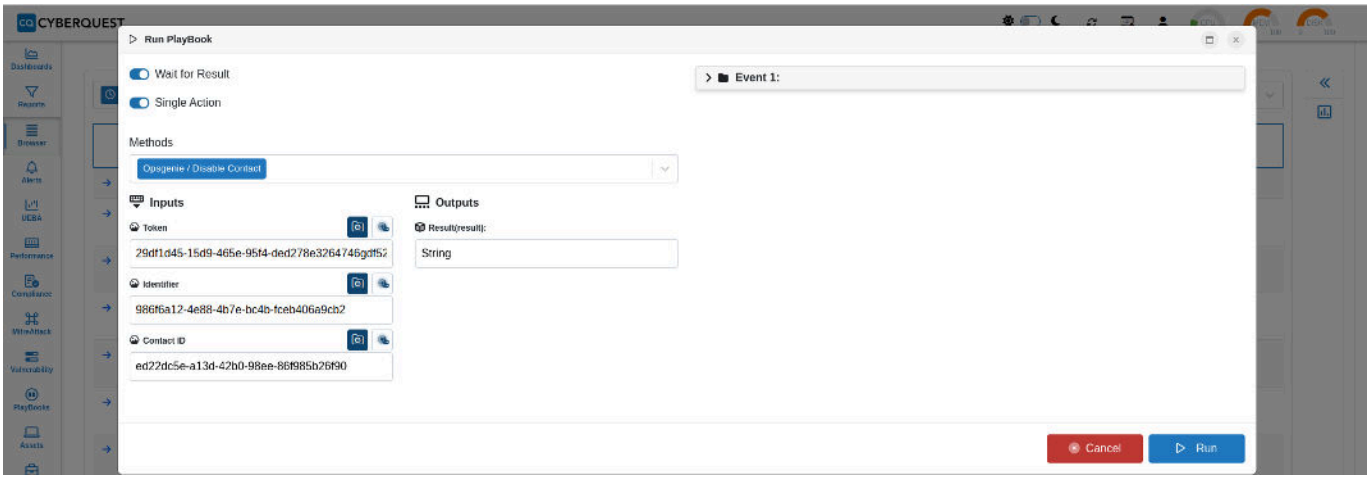


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Identifier (is required)	Identifier of the user to be searched
Contact ID (is required)	Id of the contact

Outputs	Description
Result (result)	The result of the API call

Opsgenie/Disable Contact method

Disable the contact of the user.

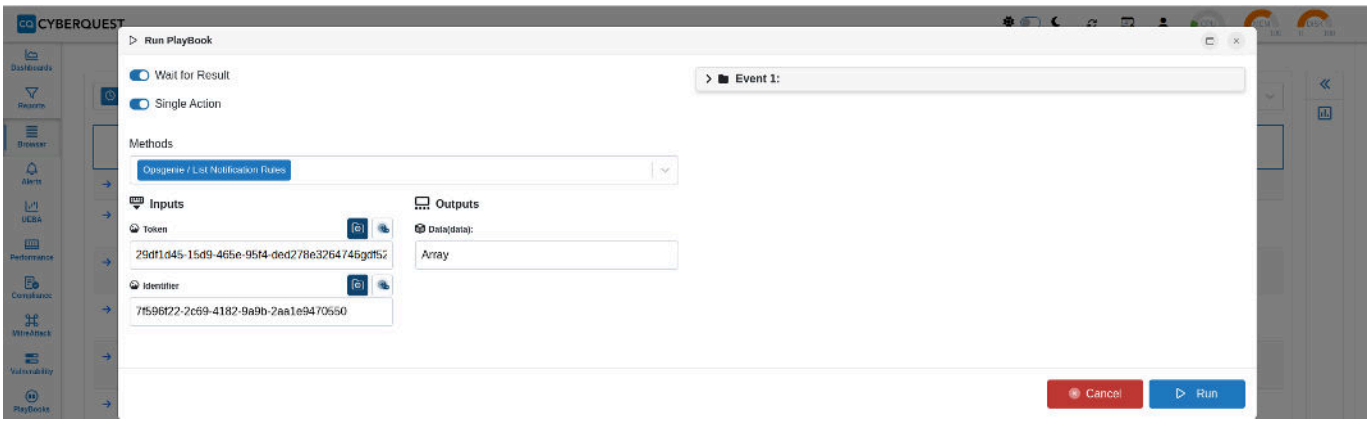


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Identifier (is required)	Identifier of the user to be searched
Contact ID (is required)	Id of the contact

Outputs	Description
Result (result)	The result of the API call

Opsgenie/List Notification Rules method

Returns list of notification rules.

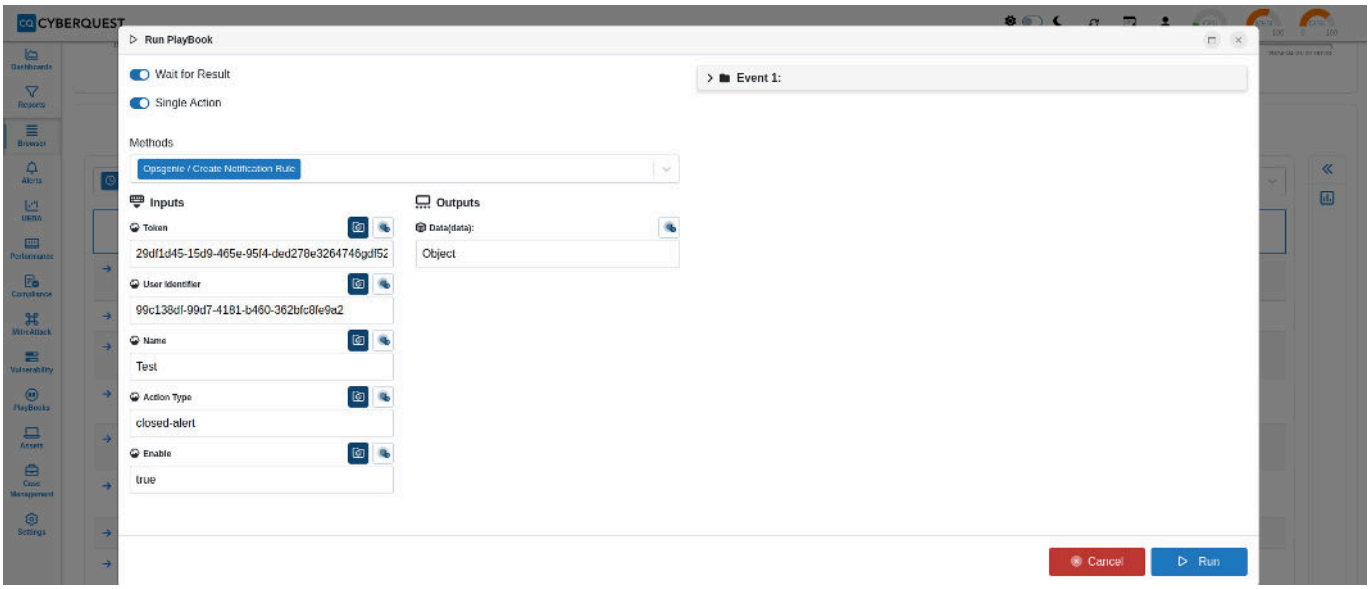


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Identifier (is required)	Identifier of the user to be searched

Outputs	Description
Data (data)	The result of the API call

Opsgenie/Create Notification Rule method

Returns list of notification rules.

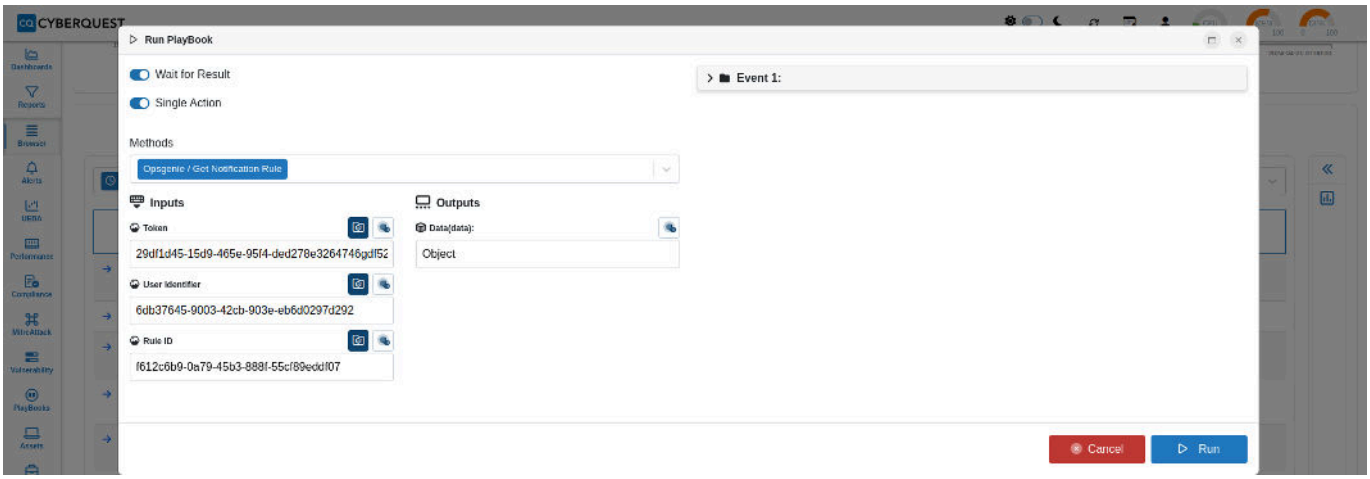


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
User Identifier (is required)	Identifier of the user for this notification rule. You should provide either id or username of the user
Name (is required)	Name of the notification rule.
Action Type (is required)	Type of the action that notification rule will have. This parameter should be one of create-alert, acknowledged-alert, closed-alert, assigned-alert, add-note, schedule-start, schedule-end and incoming-call-routing.If actionType is scheduleStart or scheduleEnd, notificationTime is mandatory
Enable (is required)	If notification rule will be enabled or not when it is created

Outputs	Description
Data (data)	Details about the new created notification rule

Opsgenie/Get Notification Rule method

Returns notification rule with given id.

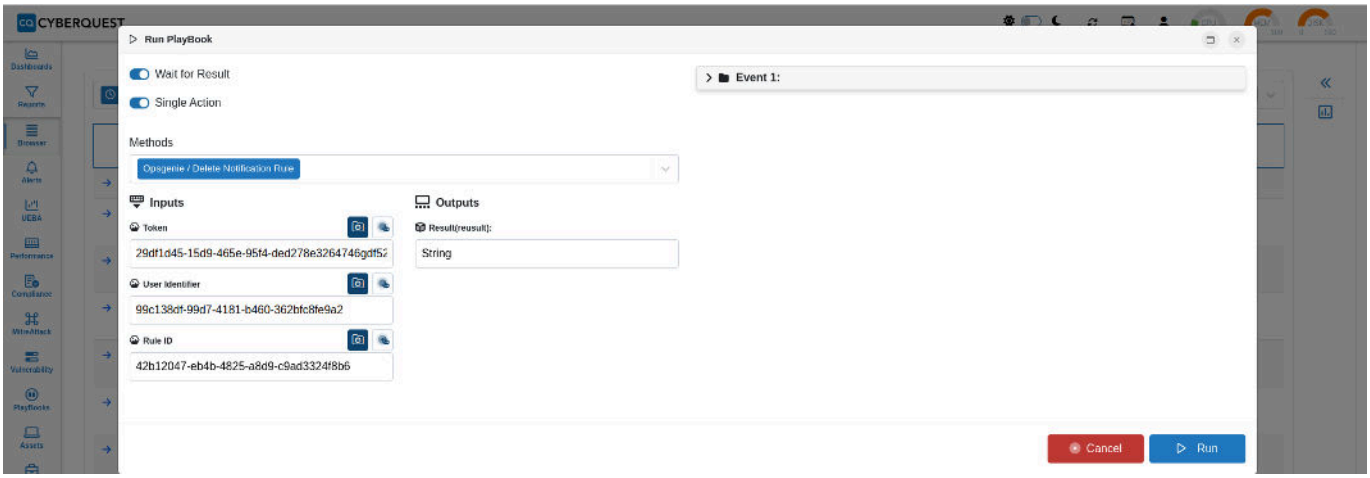


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
User Identifier (is required)	Identifier of the user for this notification rule. You should provide either id or username of the user
Rule ID (is required)	Id of the notification rule

Outputs	Description
Data (data)	The result of the API call

Opsgenie/Delete Notification Rule method

Deletes a notification rule with given notification rule id.

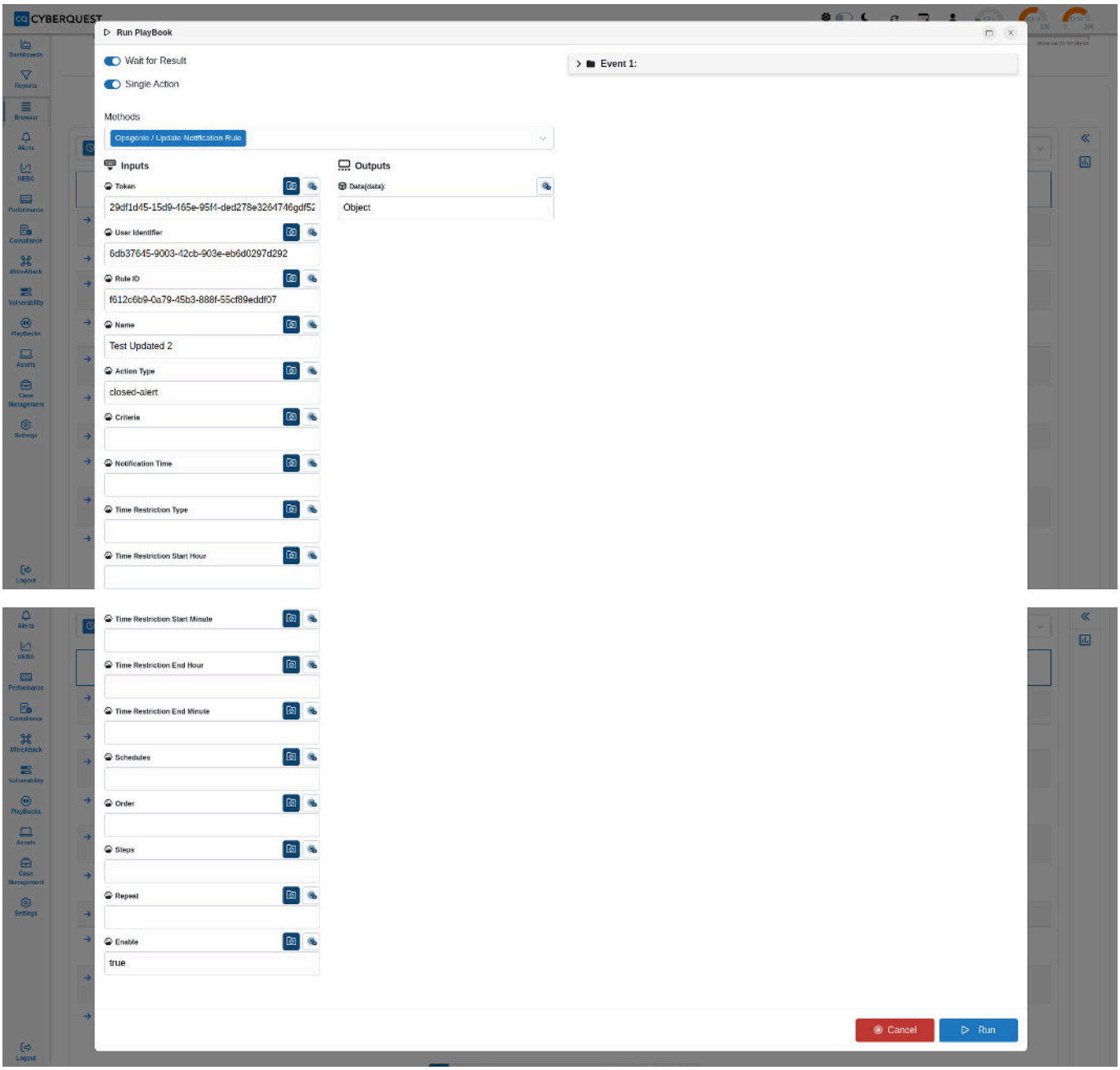


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
User Identifier (is required)	Identifier of the user for this notification rule. You should provide either id or username of the user
Rule ID (is required)	Id of the notification rule

Outputs	Description
Result (reusult)	The result of the API call

Opsgenie/Update Notification Rule method

Deletes a notification rule with given notification rule id.

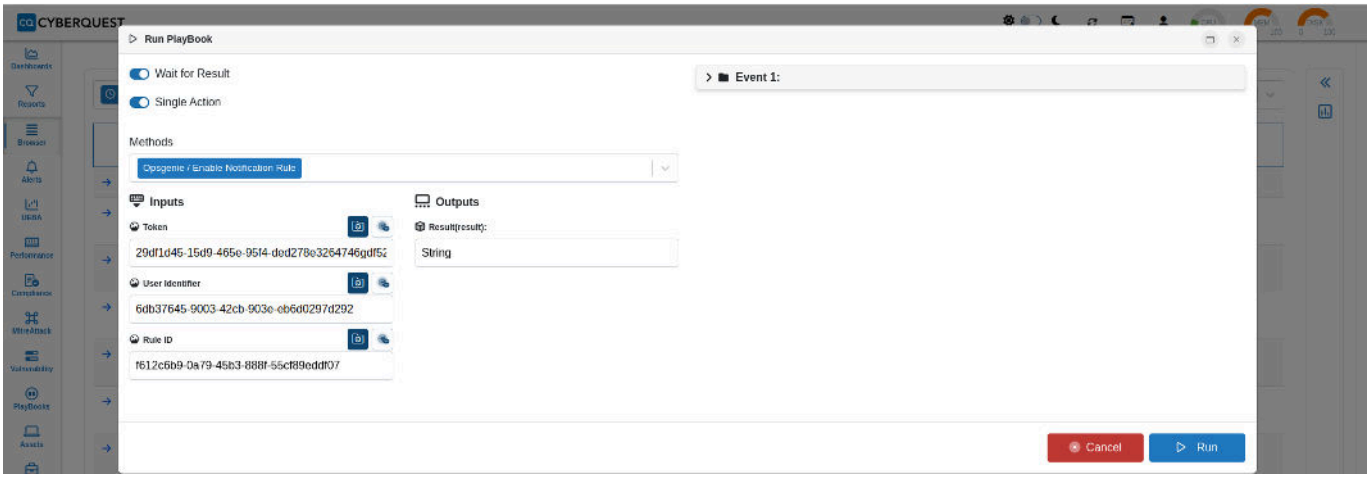

CYBERQUEST
Run PlayBook
Wait for Result
Single Action
Methods
Opsgenie / Update Notification Rule
Inputs
Token
29df1d45-15d9-465e-95f4-ded278e32647f6gdf52
User Identifier
6db37645-9003-42cb-903e-eb6d0297d292
Rule ID
f612c6b9-0a79-45b3-888f-55cf89eddf07
Name
Test Updated 2
Action Type
closed-alert
Criteria
Notification Time
Time Restriction Type
Time Restriction Start Hour
Outputs
Data(data):
Object
Event 1:
Time Restriction Start Minute
Time Restriction End Hour
Time Restriction End Minute
Schedules
Order
Steps
Repeat
Enable
true
Cancel
Run

Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
User Identifier (is required)	Identifier of the user for this notification rule. You should provide either id or username of the user
Rule ID (is required)	Id of the notification rule
Name (is required)	Name of the notification rule.
Action Type (is required)	Type of the action that notification rule will have. This parameter should be one of create-alert, acknowledged-alert, closed-alert, assigned-alert, add-note, schedule-start, schedule-end and incoming-call-routing.If actionType is scheduleStart or scheduleEnd, notificationTime is mandatory
Criteria	Defines the conditions that will be checked before applying notification rule and type of the operations that will be applied on conditions. Default value is matching all notification rules.
Notification Time	List of Time Periods that notification for schedule start/end will be sent. This parameter should be one of just-before, 15-minutes-ago, 1-hour-ago and 1-day-ago
Time Restriction Type	The type of time restriction
Time Restriction Start Hour	Starting hour of notification rule
Time Restriction Start Minute	Starting minute of notification rule
Time Restriction End Hour	Ending hour of notification rule
Time Restriction End Minute	Ending minute of notification rule
Schedules	This field is valid for Schedule Start/End rules. It can be list of schedules that notification rule will be applied when on call of that schedule starts/ends. This field shall only be populated with the specified users schedules.
Order	he order of the notification rule within the notification rules with the same action type. order value is actually the index of the notification rule whose minimum value is 0 and whose maximum value is n-1 (number of notification rules with the same action type is n)
Steps	List of steps that will be added to notification rule.
Repeat	The amount of time in minutes that notification steps will be repeatedly apply.
Enable (is required)	If notification rule will be enabled or not when it is created

Outputs	Description
Data (data)	Details about the updated notification rule

Opsgenie/Enable Notification Rule method

Enable notification rule.

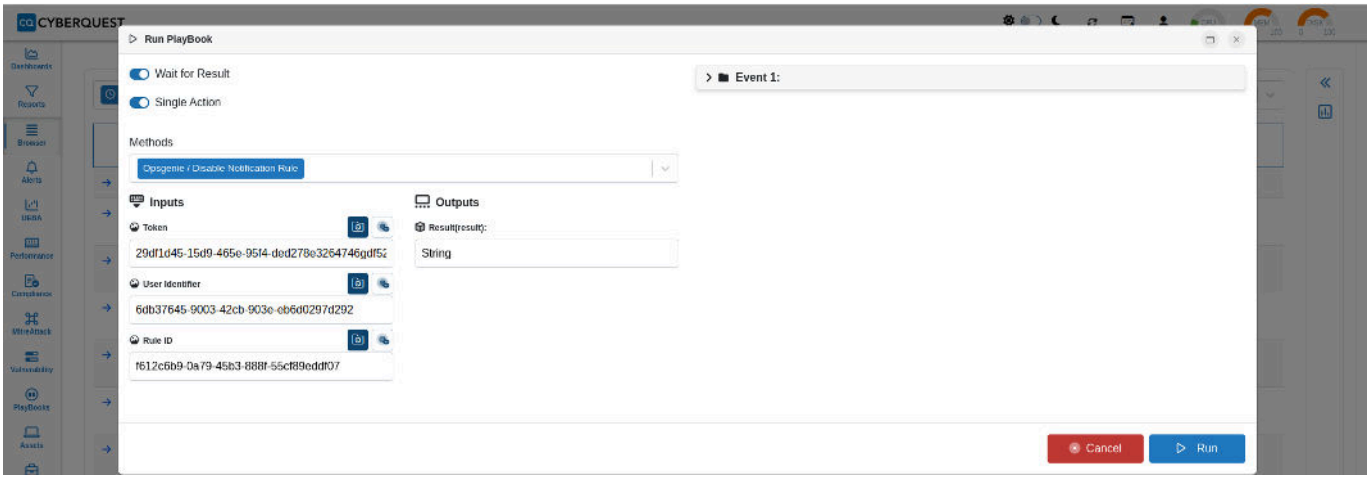


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
User Identifier (is required)	Identifier of the user for this notification rule. You should provide either id or username of the user
Rule ID (is required)	Id of the notification rule

Outputs	Description
Result (result)	The result of the API call

Opsgenie/Disable Notification Rule method

Enable notification rule.

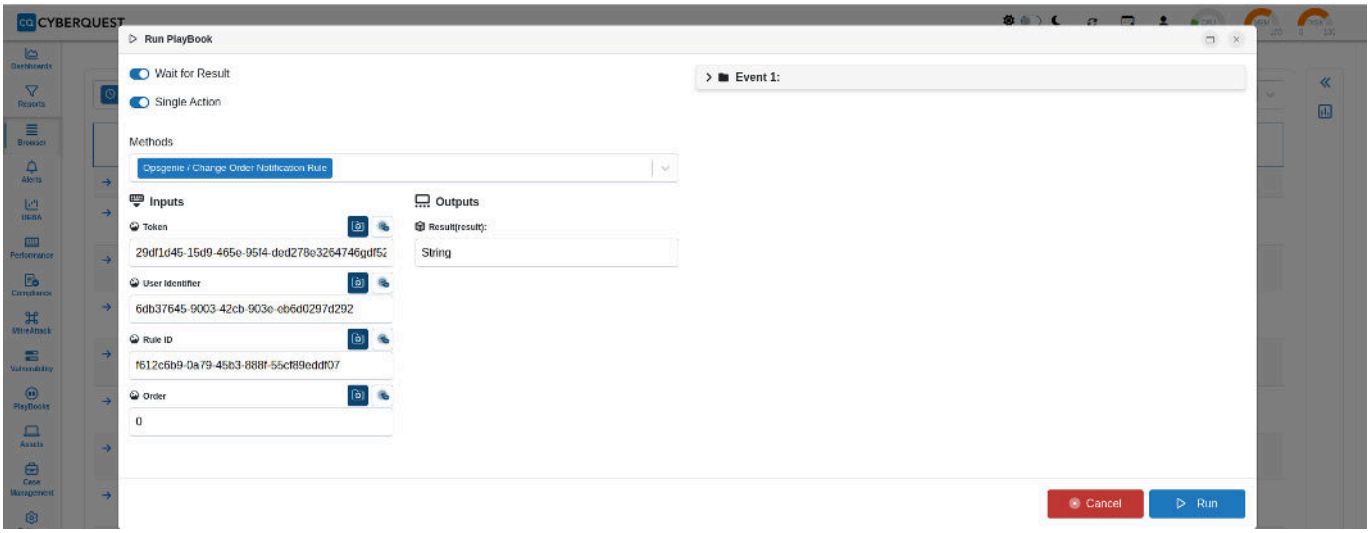


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
User Identifier (is required)	Identifier of the user for this notification rule. You should provide either id or username of the user
Rule ID (is required)	Id of the notification rule

Outputs	Description
Result (result)	The result of the API call

Opsgenie/Change Order Notification Rule method

Changes order of a notification rule with given notification rule id.

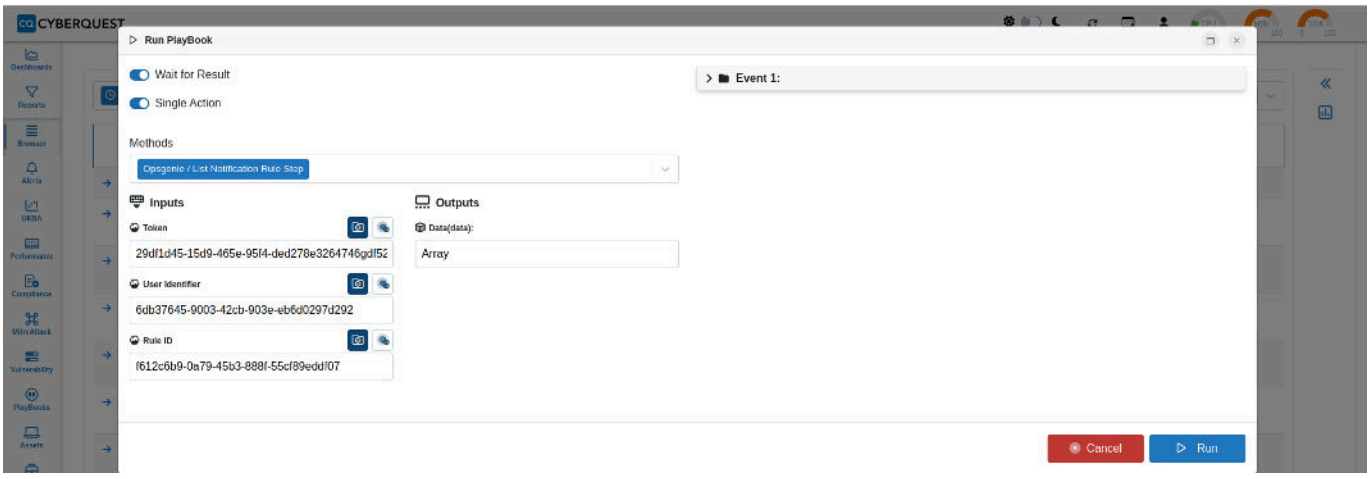


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
User Identifier (is required)	Identifier of the user for this notification rule. You should provide either id or username of the user
Rule ID (is required)	Id of the notification rule
Order (is required)	The order of the rule

Outputs	Description
Result (result)	The result of the API call

Opsgenie/List Notification Rule Step method

Returns list of notification rule steps.

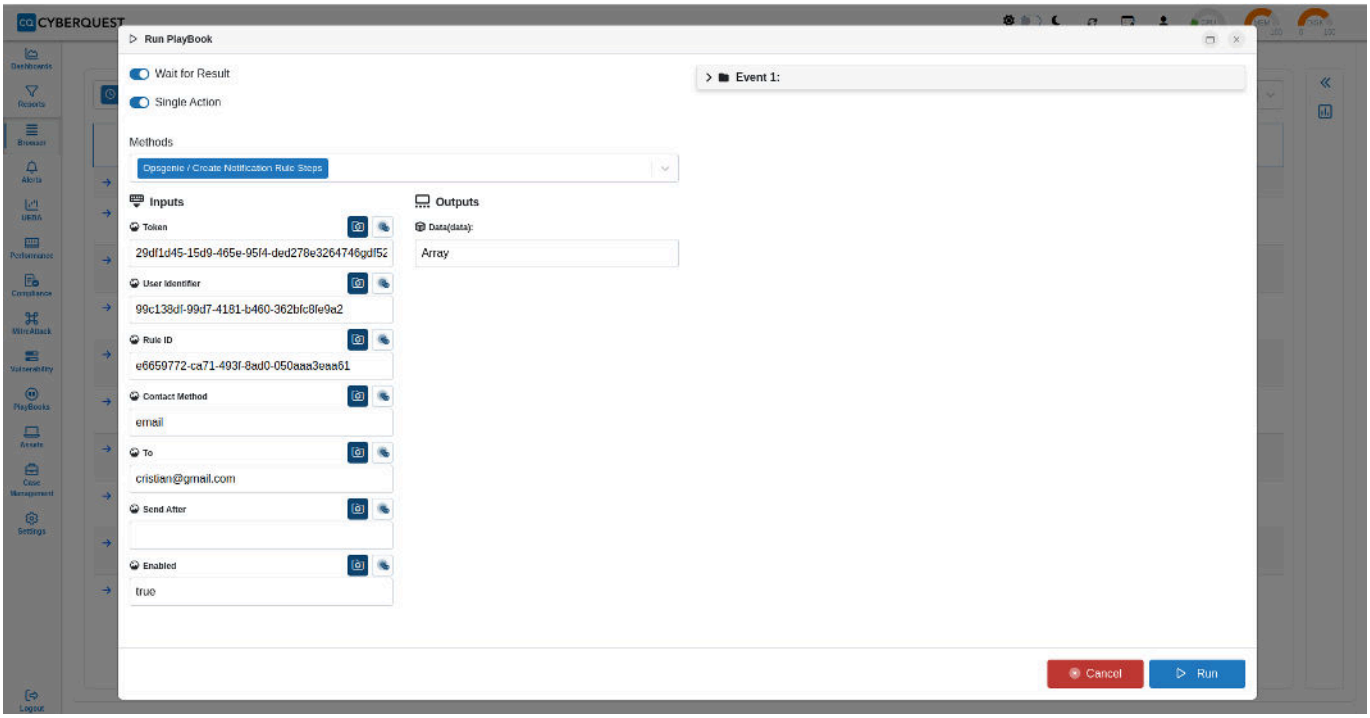


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
User Identifier (is required)	Identifier of the user for this notification rule. You should provide either id or username of the user
Rule ID (is required)	Id of the notification rule

Outputs	Description
Data (data)	The results of the API call

Opsgenie/Create Notification Rule Steps method

Returns list of notification rule steps.

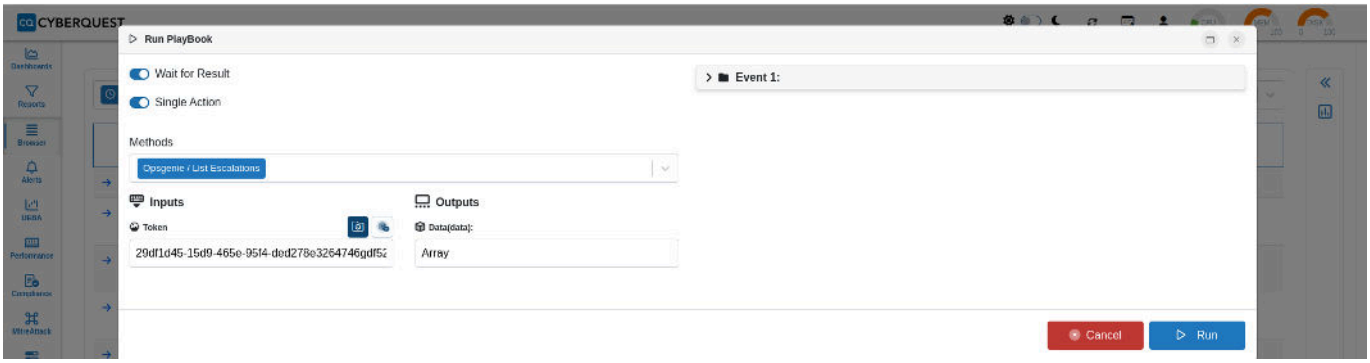


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
User Identifier (is required)	Identifier of the user for this notification rule. You should provide either id or username of the user
Rule ID (is required)	Id of the notification rule
Contact Method (is required)	Method how to get on contact
To (is required)	Recipient
Send After	Time period (in minute) when notification will be sent after. Valid and Mandatory only for New Alert and Assigned Alert notification rules. sendAfter parameter should be given as an object which has a timeAmount field that takes amount as minutes.
Enabled (is required)	Specifies whether given step will be enabled or not when it is created

Outputs	Description
Data (data)	Details about notification rule steps created

Opsgenie/List Escalations method

Returns list of escalations.

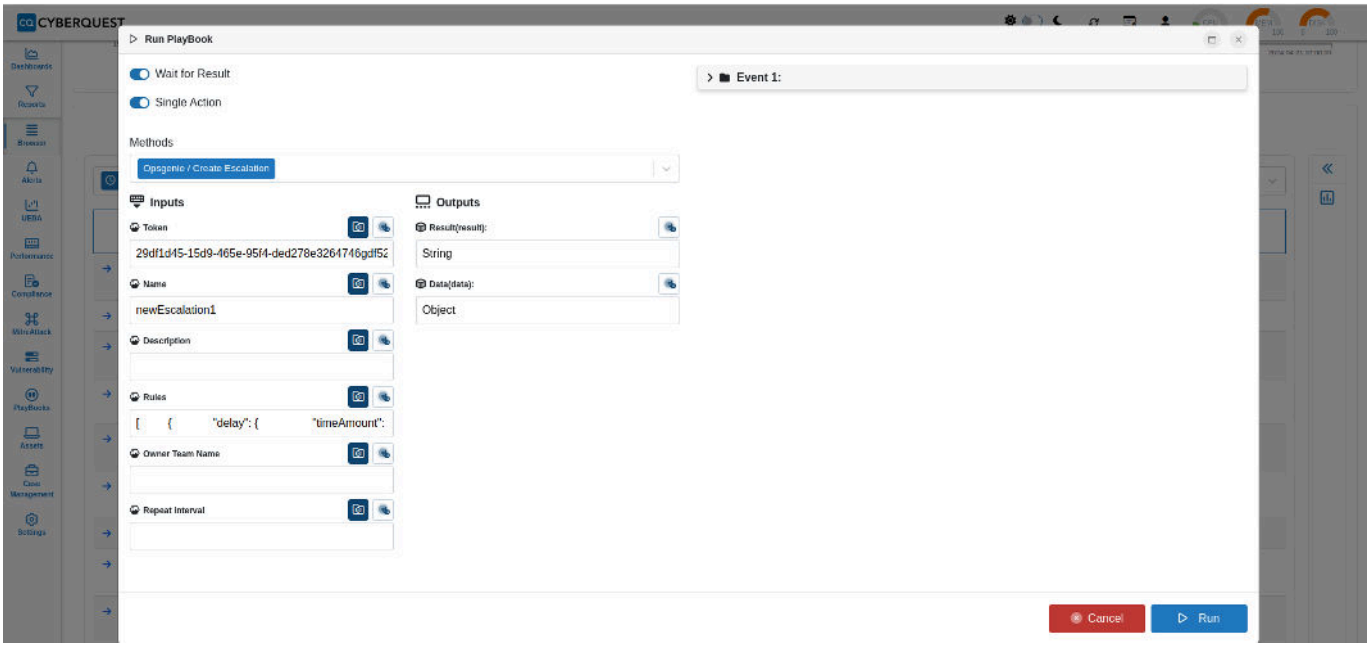


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.

Outputs	Description
Data (data)	The results of the API call

Opsgenie/Create Escalation method

Creates a new escalation.

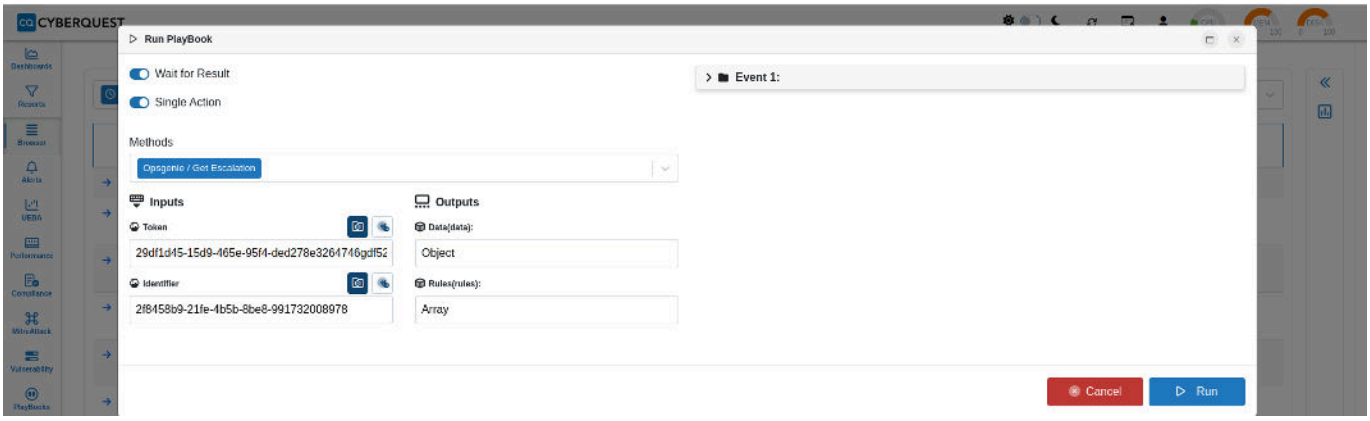


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Name (is required)	Name of the escalation
Description	Description of the escalation
Rules (is required)	List of the escalation rules.
Owner Team Name	Owner team of the escalation, consisting id and/or name of the owner team
Repeat interval	

Outputs	Description
Result (result)	The result of the API call
Data (data)	Details about the new created escalation

Opsgenie/Get Escalation method

Returns escalation with given id or name.

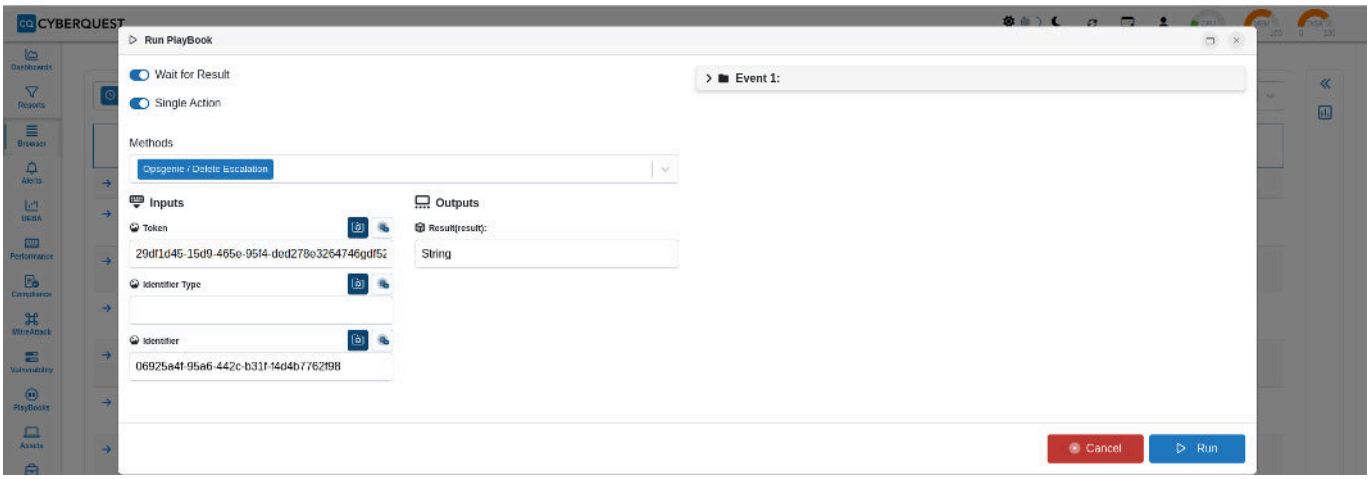


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Identifier (is required)	Identifier of the escalation

Outputs	Description
Data (data)	Details about escalation
Rules (rules)	A list of rules used by escalation

Opsgenie/Delete Escalation method

Deletes an escalation using escalation id or name.

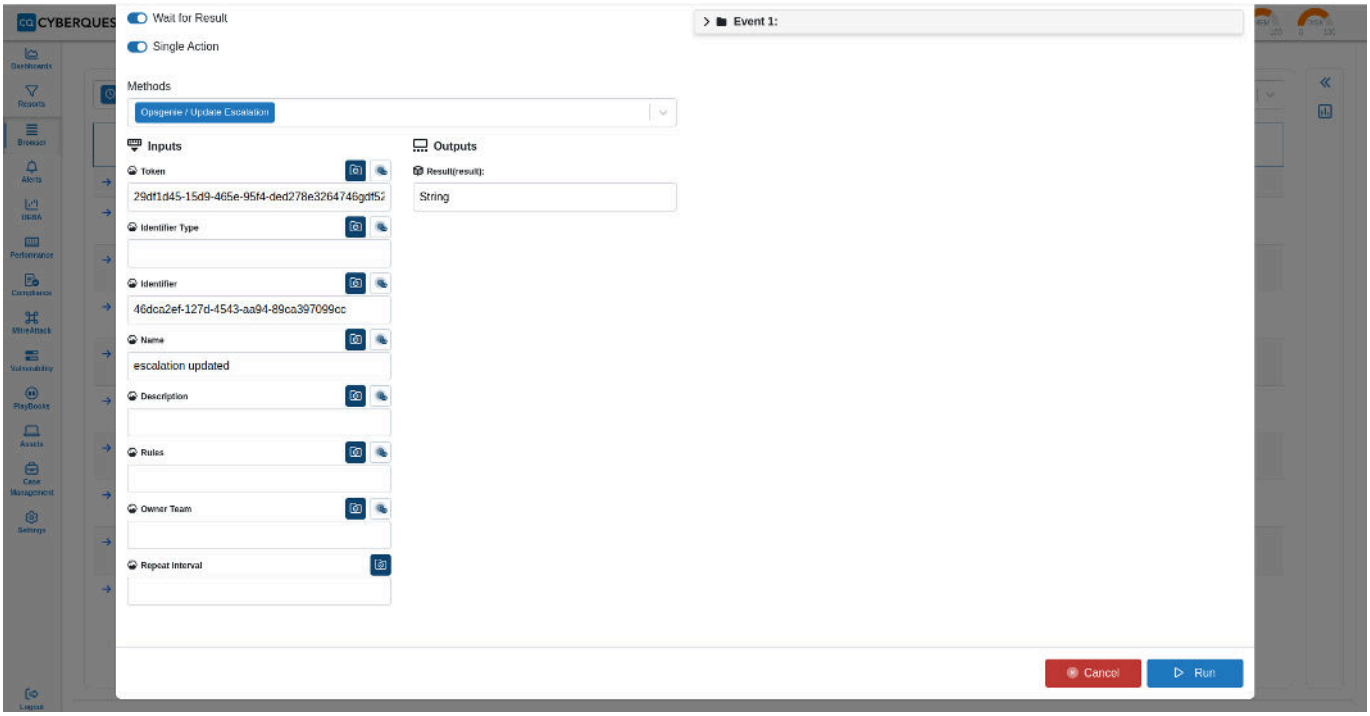


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Identifier Type	Type of the identifier that is provided as an in-line parameter. Possible values are id and name. Default value is id
Identifier (is required)	Identifier of the escalation

Outputs	Description
Result (result)	The result of the API call

Opsgenie/Update Escalation method

Updates the escalation using escalation id or name.

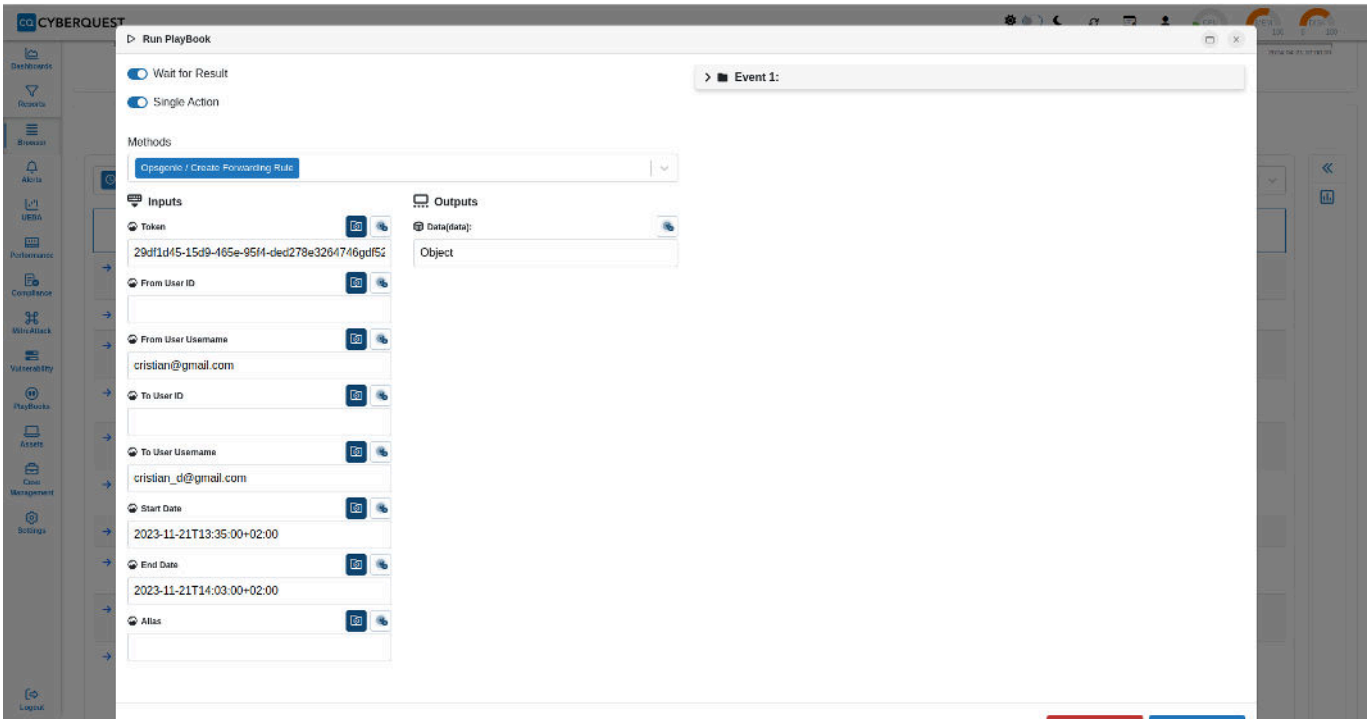


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Identifier Type	Type of the identifier that is provided as an in-line parameter. Possible values are id and name. Default value is id
Identifier	Identifier of the escalation
Name	Name of the escalation
Description	Description of the escalation
Rules	List of the escalation rules.
Owner Team	Owner team of the escalation, consisting id and/or name of the owner team
Repeat interval	

Outputs	Description
Result (result)	The result of the API call

Opsgenie/Create Forwarding Rule method

Creates a new forwarding rule.

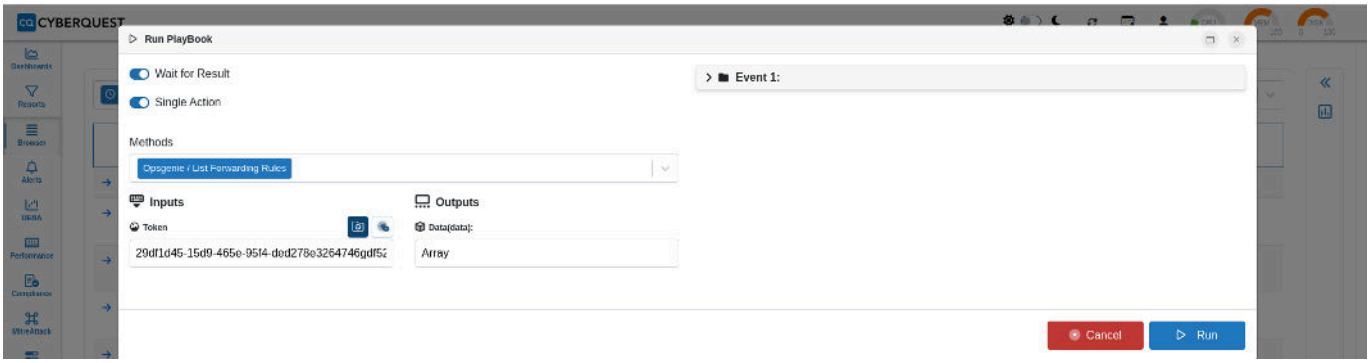


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
From User ID	The user object of user whose notifications will be forwarded. From User Id or Username Required!
From User Username	The user object of user whose notifications will be forwarded.From User Id or Username Required!
To User ID	The user object of user who will receive the forwarded notifications.From User Id or Username Required!
To User Username	The user object of user who will receive the forwarded notifications.From User Id or Username Required!
Start Date (is required)	The date and time for forwarding will start, which takes a date format as (yyyy-MM-dd T HH:mm:ssZ) (e.g. 2017-01-15T08:00:00+02:00)
End Date (is required)	The date and time for forwarding will end, which takes a date format as (yyyy-MM-dd T HH:mm:ssZ) (e.g. 2017-01-15T08:00:00+02:00)
Alias	A user defined identifier for the forwarding rule. There can be only one forwarding rule with the same alias. Provides ability to assign a known id and later use this id to perform additional actions such as update the rule, etc.

Outputs	Description
Data (data)	Details about the new created team forwarding rule

Opsgenie/List Forwarding Rules method

Returns list of forwarding rules.

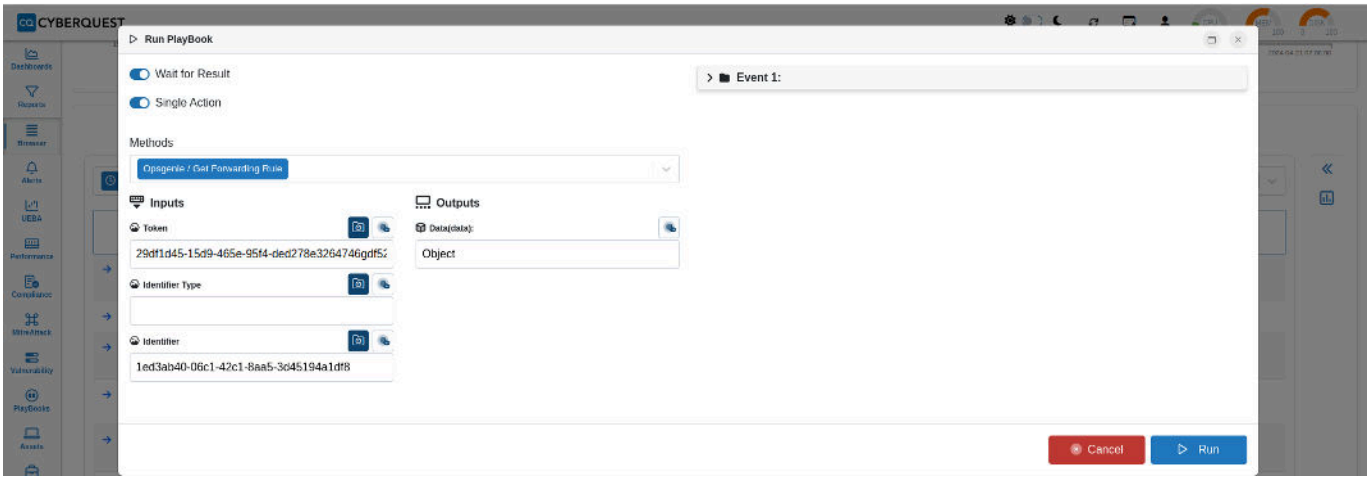


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.

Outputs	Description
Data (data)	The results of the API call

Opsgenie/Get Forwarding Rule method

Returns forwarding rule with given id or alias.

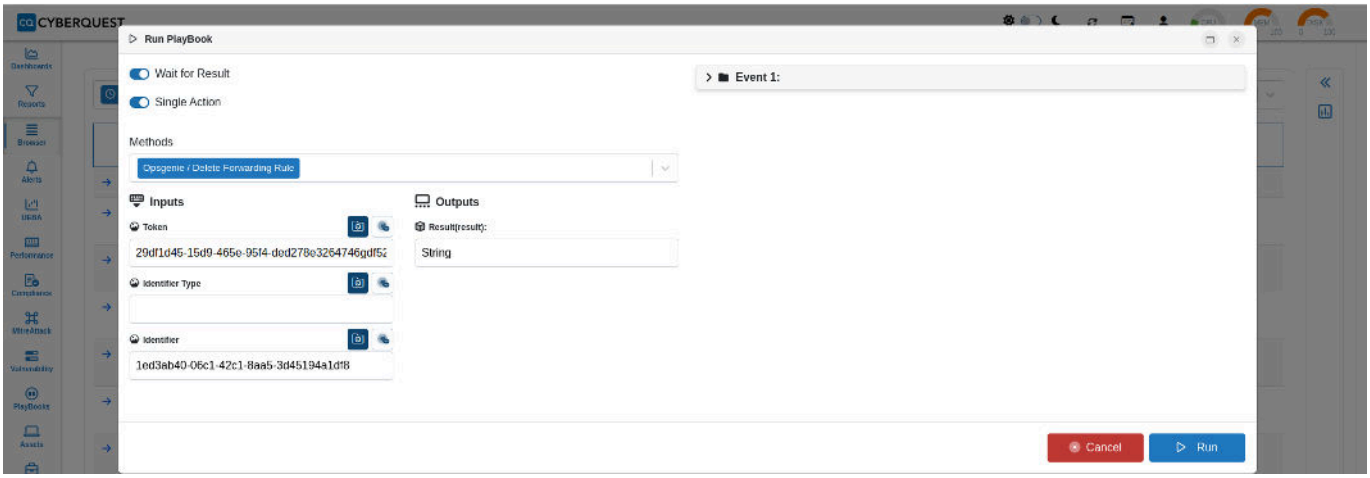


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Identifier Type	Type of the identifier that is provided as an in-line parameter. Possible values are id and alias. Default value is id
Identifier (is required)	Identifier of the forwarding rule

Outputs	Description
Data (data)	Details about the forwarding rule

Opsgenie/Delete Forwarding Rule method

Deletes forwarding rule with given identifier.

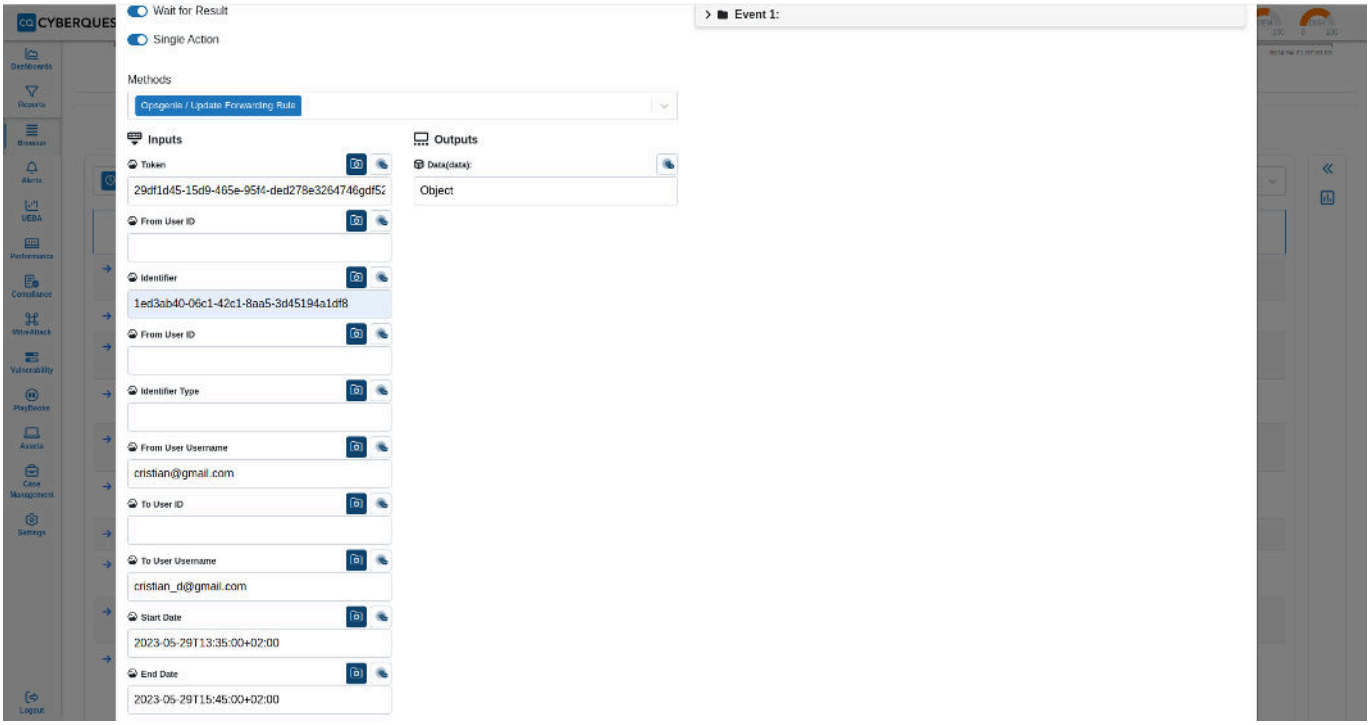


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Identifier Type	Type of the identifier that is provided as an in-line parameter. Possible values are id and alias. Default value is id
Identifier (is required)	Identifier of the forwarding rule

Outputs	Description
Result (result)	The result of the API call

Opsgenie/Update Forwarding Rule method

Update forwarding rule with given rule id or alias.

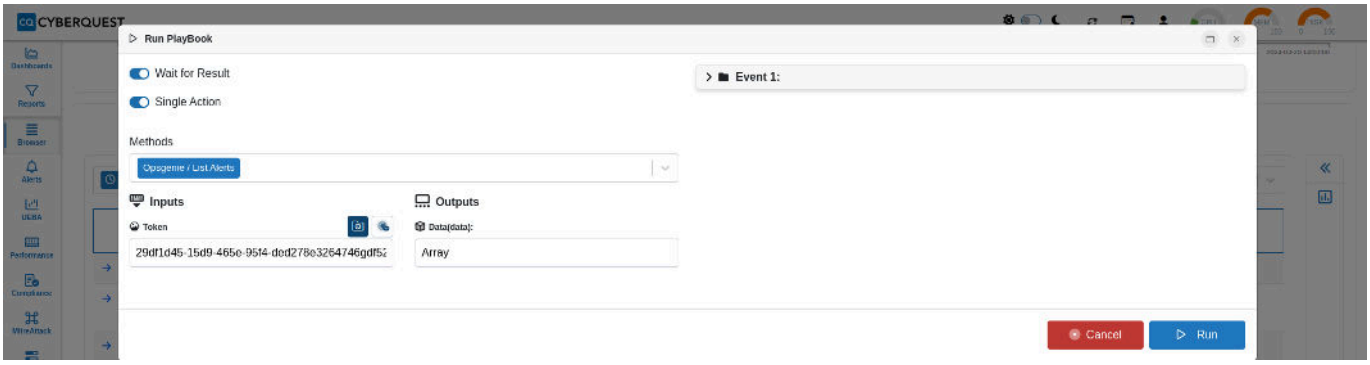


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
From User ID	The user object of user whose notifications will be forwarded. From User Id or Username Required!
Identifier (is required)	Identifier of the forwarding rule
From User ID	The user object of user whose notifications will be forwarded. From User Id or Username Required!
Identifier Type	Type of the identifier that is provided as an in-line parameter. Possible values are id and alias. Default value is id
From User Username	The user object of user whose notifications will be forwarded.From User Id or Username Required!
To User ID	The user object of user who will receive the forwarded notifications.From User Id or Username Required!
To User Username	The user object of user who will receive the forwarded notifications.From User Id or Username Required!
Start Date (is required)	The date and time for forwarding will start, which takes a date format as (yyyy-MM-dd T HH:mm:ssZ) (e.g. 2017-01-15T08:00:00+02:00)
End Date (is required)	The date and time for forwarding will end, which takes a date format as (yyyy-MM-dd T HH:mm:ssZ) (e.g. 2017-01-15T08:00:00+02:00)

Outputs	Description
Data (data)	Details about the updated forwarding rule

Opsgenie/List Alerts method

List all alerts.

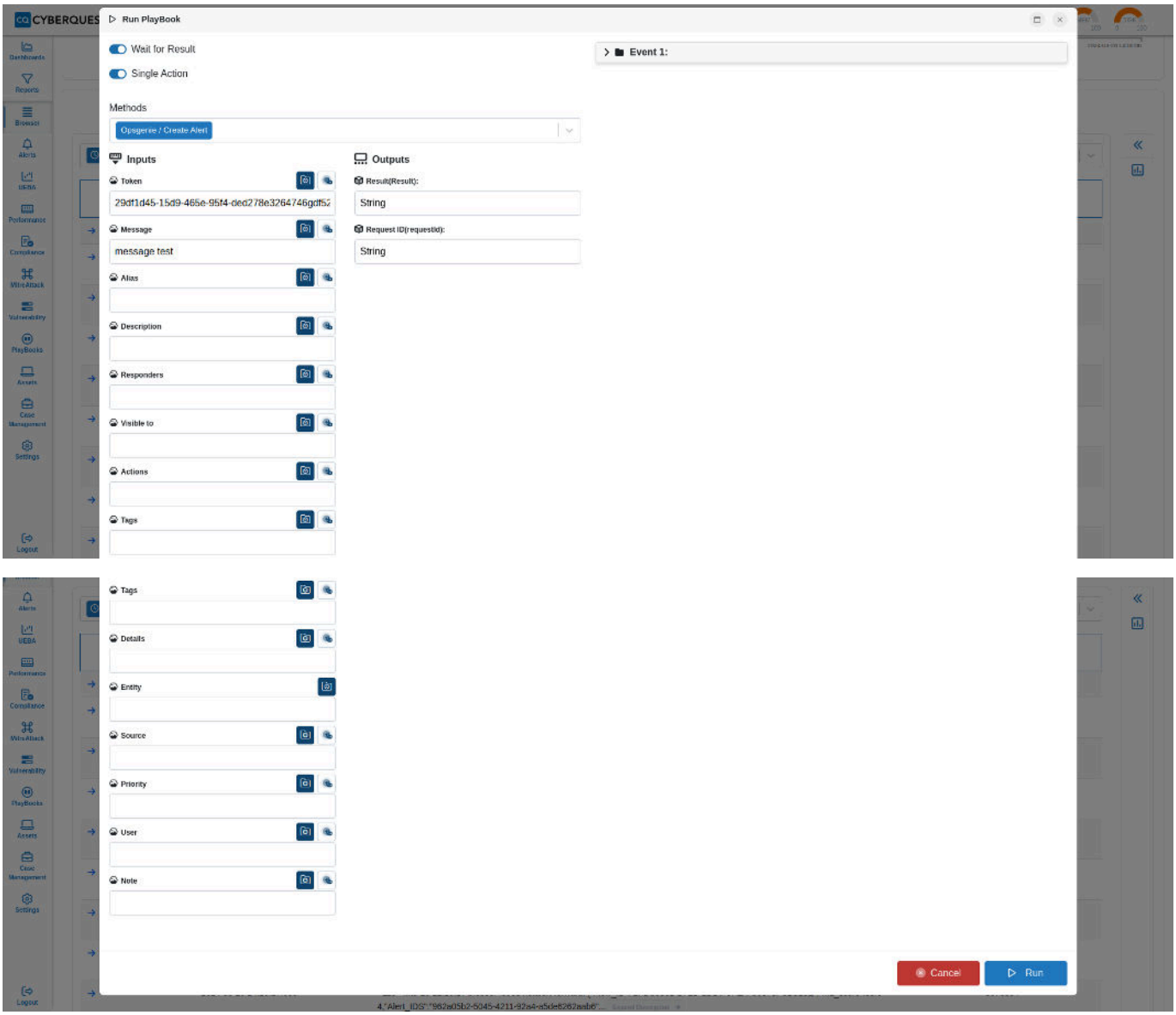


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.

Outputs	Description
Data (data)	The results of the API call

Opsgenie/Create Alert method

Create Alert.

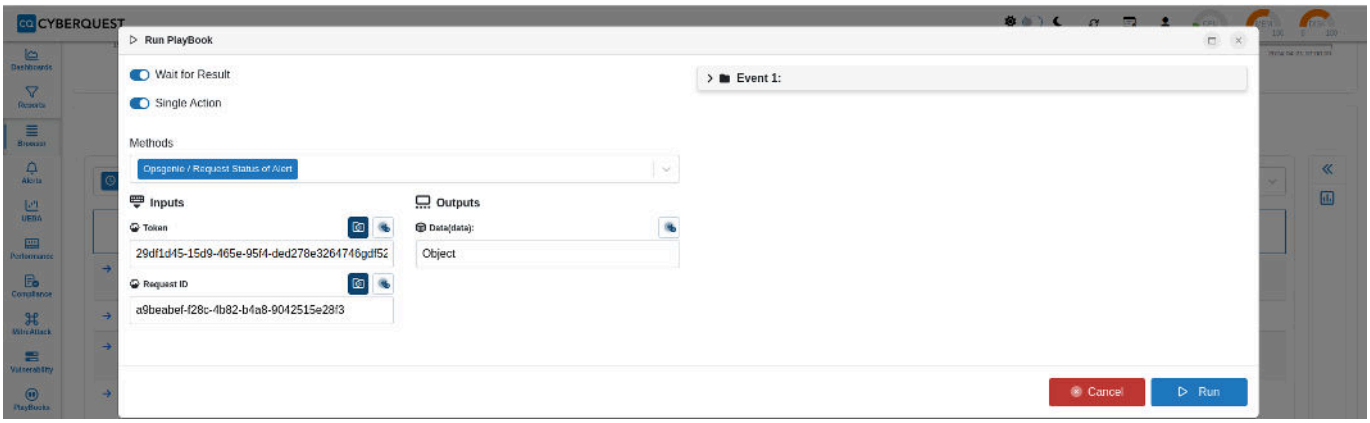

Run PlayBook
Wait for Result
Single Action
Methods
Opsgenie / Create Alert
Inputs
Outputs
Token
29df1d45-15d9-465e-95f4-ded278e3264746gdf52
Message
message test
Alias
Description
Responders
Visible to
Actions
Tags
Result(Result):
String
Request ID(requestId):
String
Event 1:
Tags
Details
Entity
Source
Priority
User
Note
Cancel
Run

Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Message (is required)	Message of the alert
Alias	Client-defined identifier of the alert
Description	Description field of the alert that is generally used to provide a detailed information about the alert
Responders	Teams, users, escalations and schedules that the alert will be routed to send notifications. type field is mandatory for each item, where possible values are team, user, escalation and schedule. If the API Key belongs to a team integration, this field will be overwritten with the owner team. Either id or name of each responder should be provided.You can refer below for example values.
Visible to	Teams and users that the alert will become visible to without sending any notification.type field is mandatory for each item, where possible values are team and user. In addition to the type field, either id or name should be given for teams and either id or username should be given for users. Please note: that alert will be visible to the teams that are specified withinresponders field by default, so there is no need to re-specify them within visibleTo field. You can refer below for example values.
Actions	Custom actions that will be available for the alert.
Tags	Tags of the alert
Details	Map of key-value pairs to use as custom properties of the alert.
Entity	
Source	Source field of the alert. Default value is IP address of the incoming request.
Priority	Priority level of the alert. Possible values are P1, P2, P3, P4 and P5. Default value is P3.
User	Display name of the request owner.
Note	Additional note that will be added while creating the alert.

Outputs	Description
Result (Result)	The results of the API call
Request ID (requestId)	The results of the API call

Opsgenie/Request Status of Alert method

Alert creation, deletion, and action requests are processed asynchronously to provide higher availability and scalability, therefore valid requests for those endpoints are responded to with HTTP status 202 - Accepted. The Get Request Status endpoint is used to track the status and alert details (if any) of the request whose identifier is given.

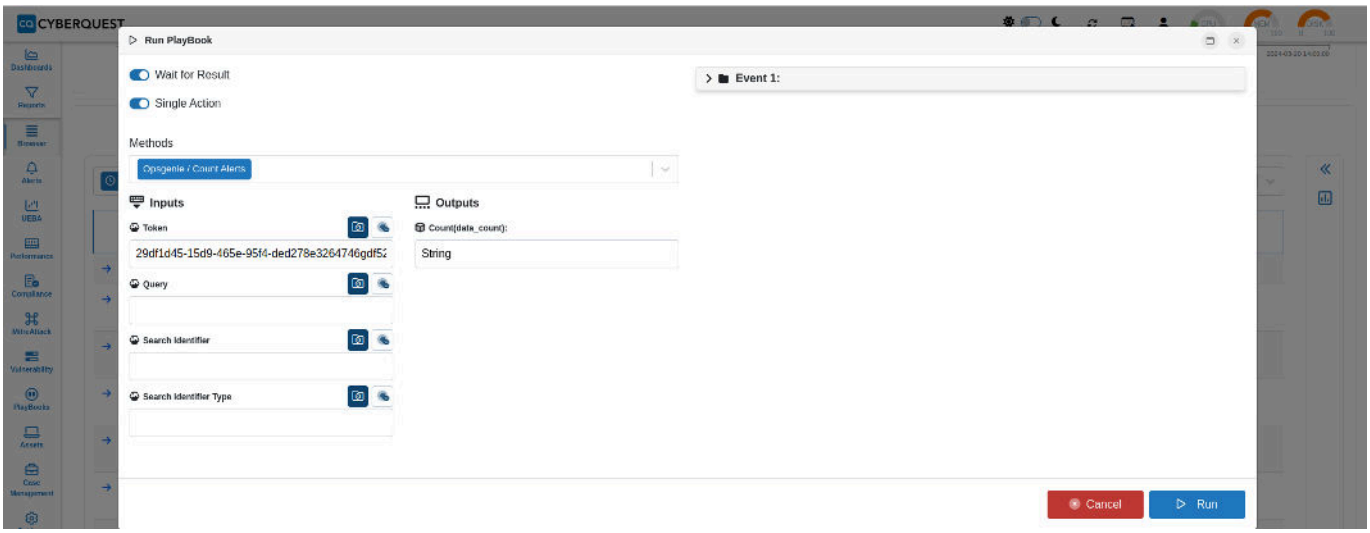


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Request ID (is required)	Universally unique identifier of the questioned request. Please note: that ID of the request was provided within response.

Outputs	Description
Data (data)	The result of the API call

Opsgenie/Count Alerts method

Count alerts request is used to count alerts in Opsgenie.

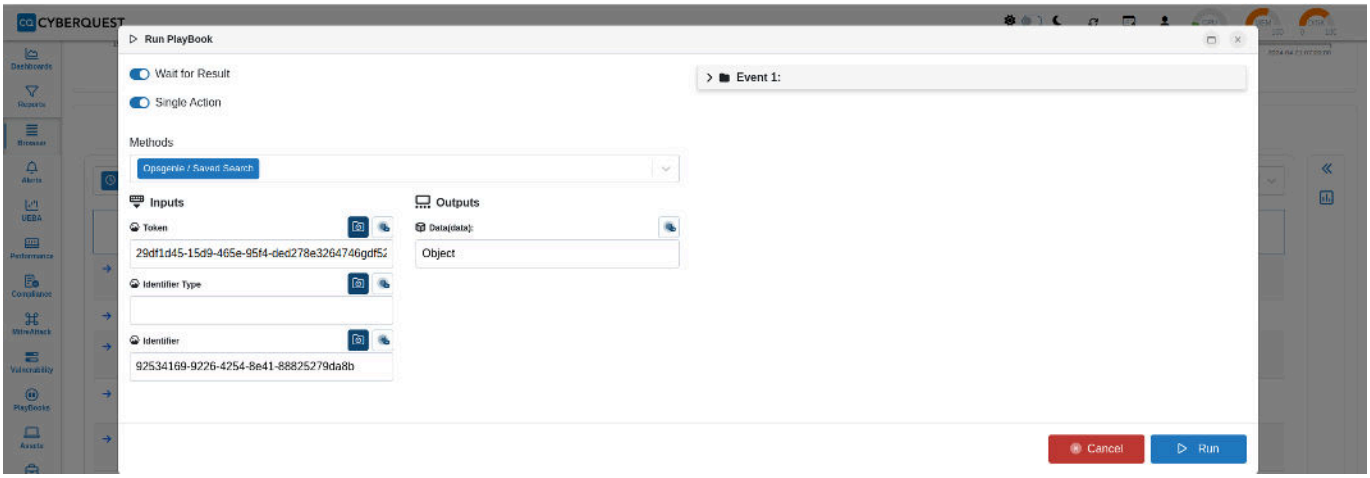


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Query	Search query to apply while filtering the alerts. You can refer Alerts Search Query Help for further information about search queries.
Search Identifier	Identifier of the saved search query to apply while filtering the alerts.
Search Identifier Type	Identifier type of the saved search query. Possible values are id and name. Default value is id. If searchIdentifier is not provided, this value is ignored.

Outputs	Description
Count (data_count)	The number Alerts

Opsgenie/Saved Search method

Get saved search for the given search identifier.

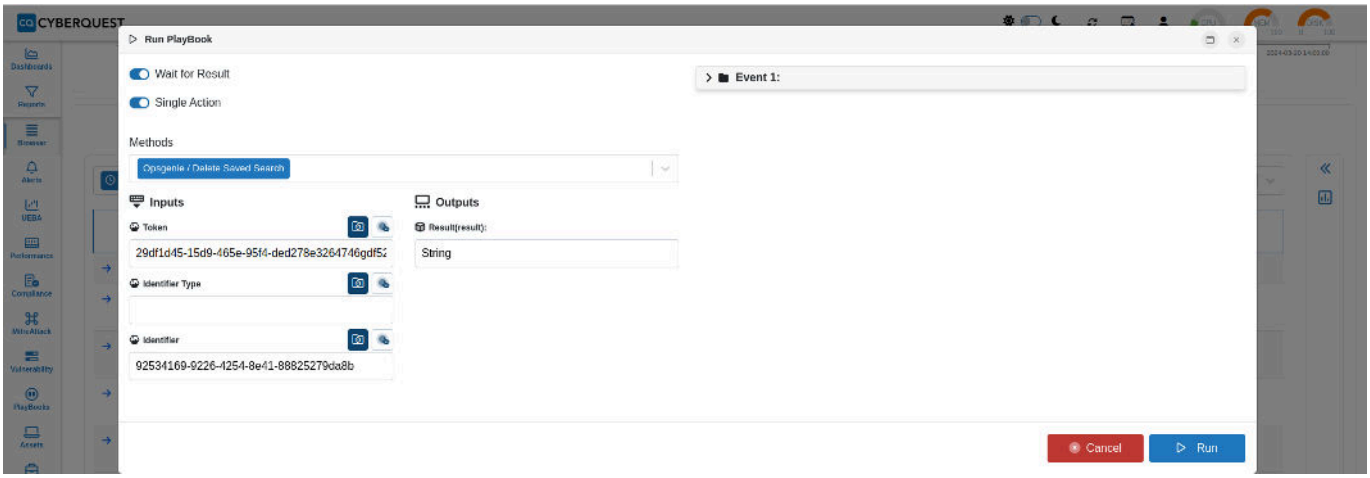


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Identifier Type	Type of the identifier that is provided as an in-line parameter. Possible values are id and name. Default value is id.
Identifier (is required)	Identifier of the saved search

Outputs	Description
Data (data)	Details about saved search

Opsgenie/Delete Saved Search method

Deletes saved search using given search identifier.

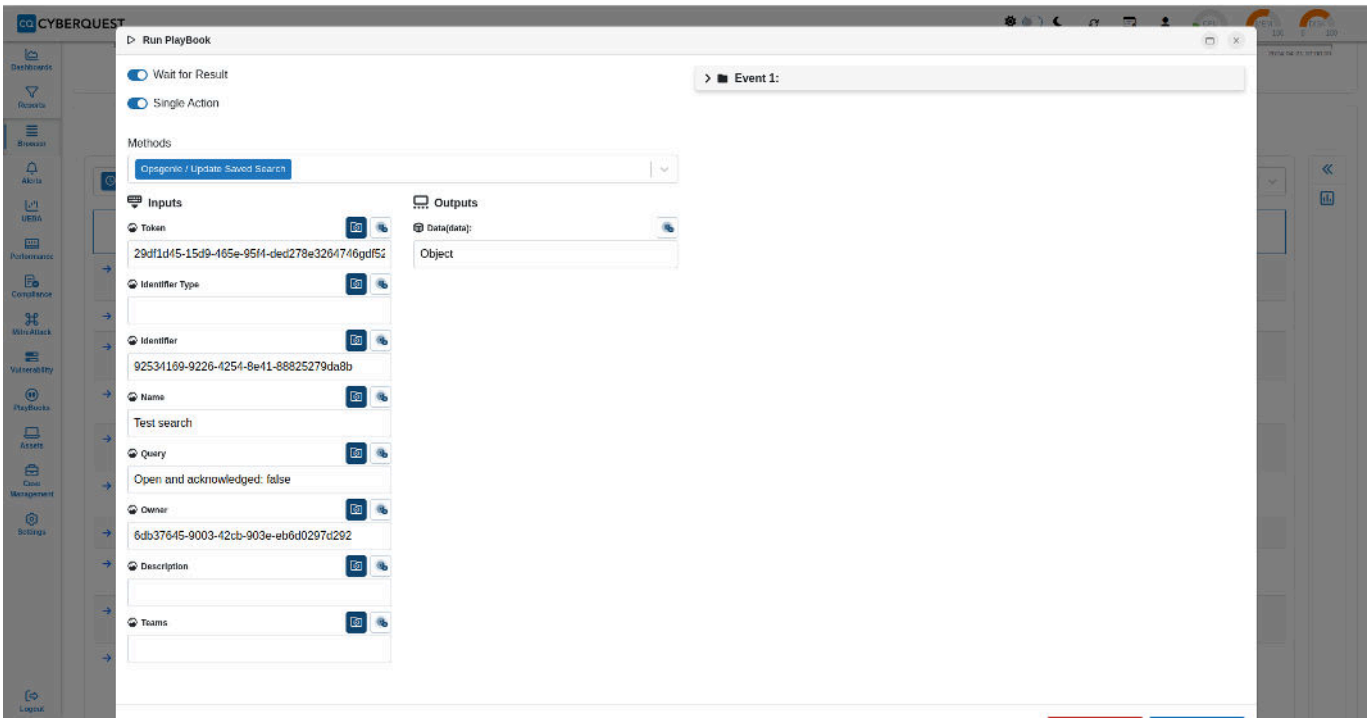


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Identifier Type	Type of the identifier that is provided as an in-line parameter. Possible values are id and name. Default value is id.
Identifier	Identifier of the saved search

Outputs	Description
Result (result	The result of the API call

Opsgenie/Update Saved Search method

Deletes saved search using given search identifier.

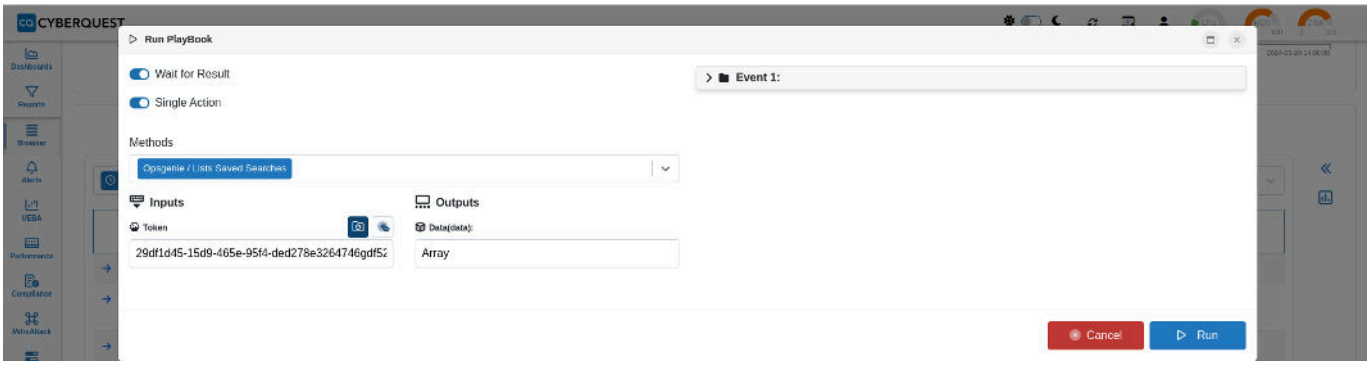


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Identifier Type	Type of the identifier that is provided as an in-line parameter. Possible values are id and name. Default value is id.
Identifier (is required)	Identifier of the saved search
Name (is required)	Unique name of the saved search.
Query (is required)	Search query to be used while filtering the alerts.
Owner (is required)	User that will be assigned as owner of the saved search. Saved searches are always accessible to their owners.
Description	Informational description of the saved search. Maximum length is 15000 characters.
Teams	Teams that saved search is assigned to. If a saved-search is assigned to at least one team, saved-search will only be accessible to the owner and members of the assigned teams. A saved-search can be assigned to at most 20 teams.

Outputs	Description
Data (data)	Details about saved search updated

Opsgenie/Lists Saved Searches method

List Saved Searches.

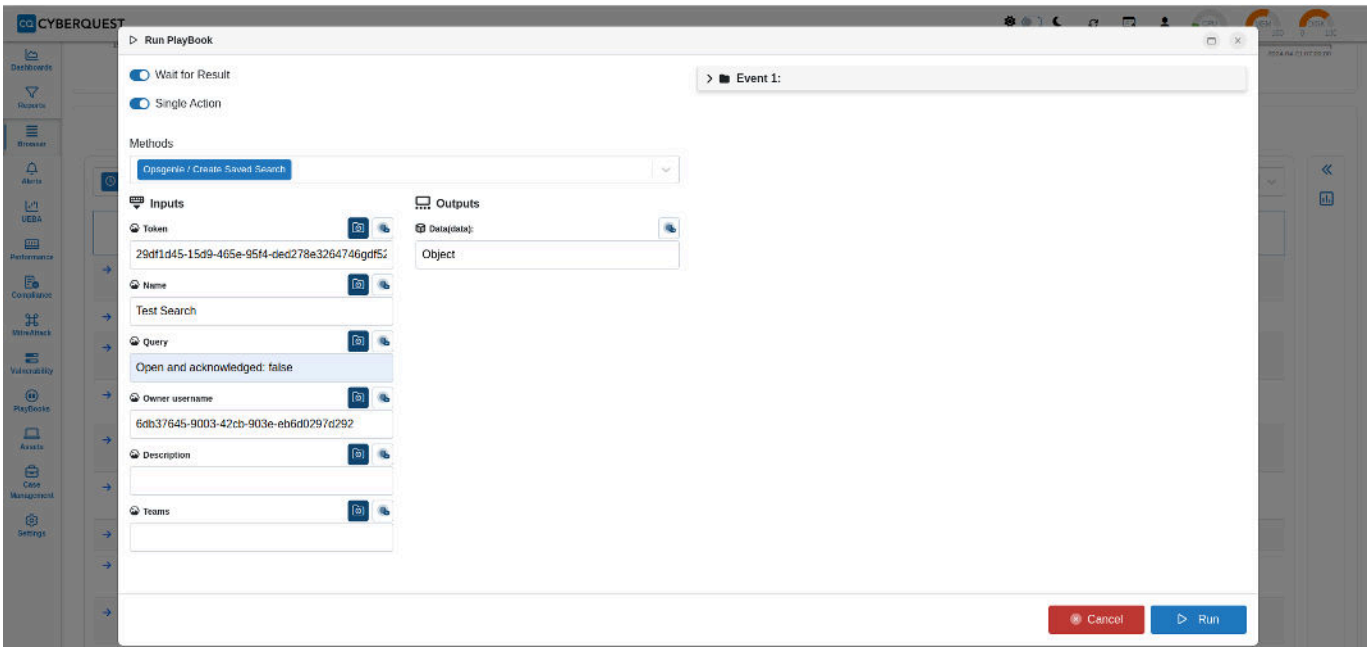


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.

Outputs	Description
Data (data)	The results of the API call

Opsgenie/Create Saved Search method

Create saved search with given fields.

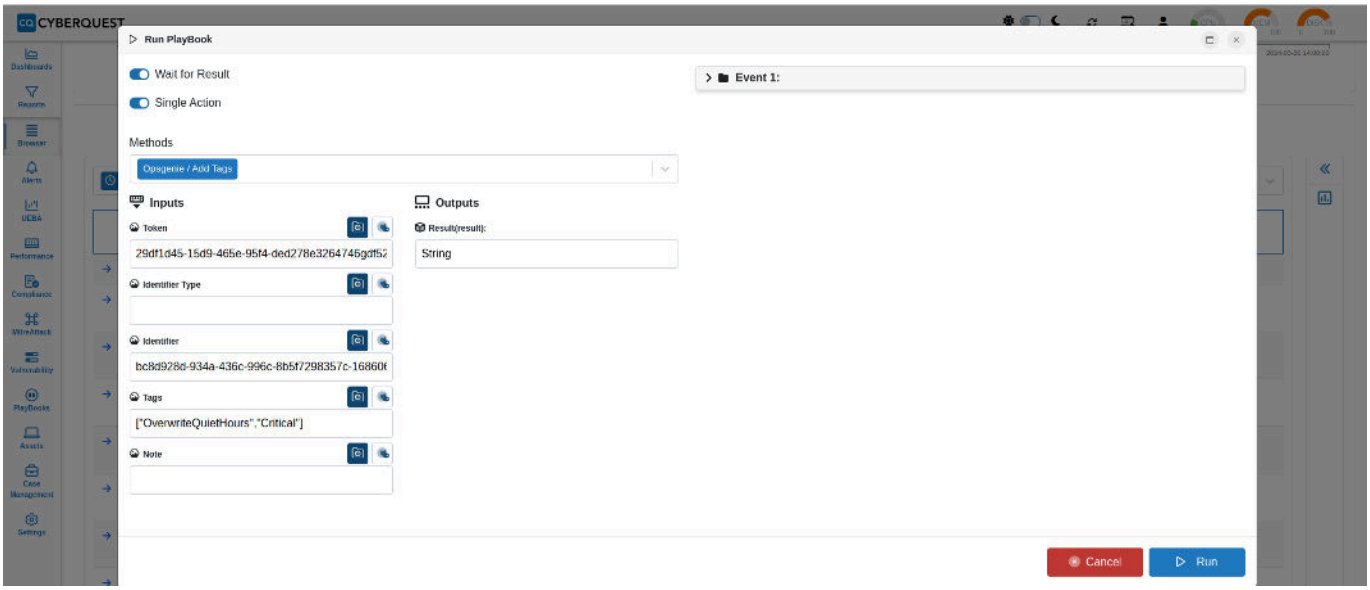


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Name (is required)	Unique name of the saved search.
Query (is required)	Search query to be used while filtering the alerts.
Owner username (is required)	User that will be assigned as owner of the saved search. Saved searches are always accessible to their owners.
Description	Informational description of the saved search. Maximum length is 15000 characters.
Teams	Teams that saved search is assigned to. If a saved-search is assigned to at least one team, saved-search will only be accessible to the owner and members of the assigned teams. A saved-search can be assigned to at most 20 teams.

Outputs	Description
Data (data)	Details about the new created saved search

Opsgenie/Add Tags method

Add tags to the alert with given identifier.

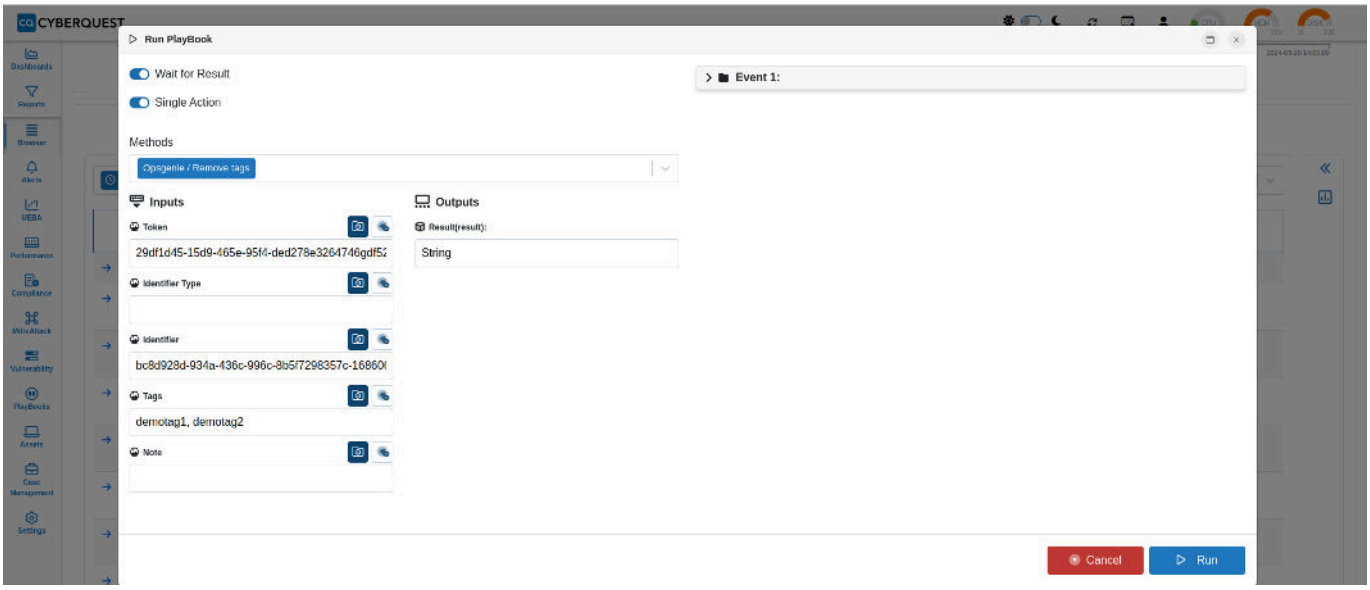


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Identifier Type	Type of the identifier that is provided as an in-line parameter. Possible values are id and name. Default value is id.
Identifier (is required)	Identifier of the alert
Tags (is required)	List of tags to add into alert
Note	Additional alert note to add

Outputs	Description
Result (result)	The result of the API call

Opsgenie/Remove tags method

Remove tags of the alert with given identifier.

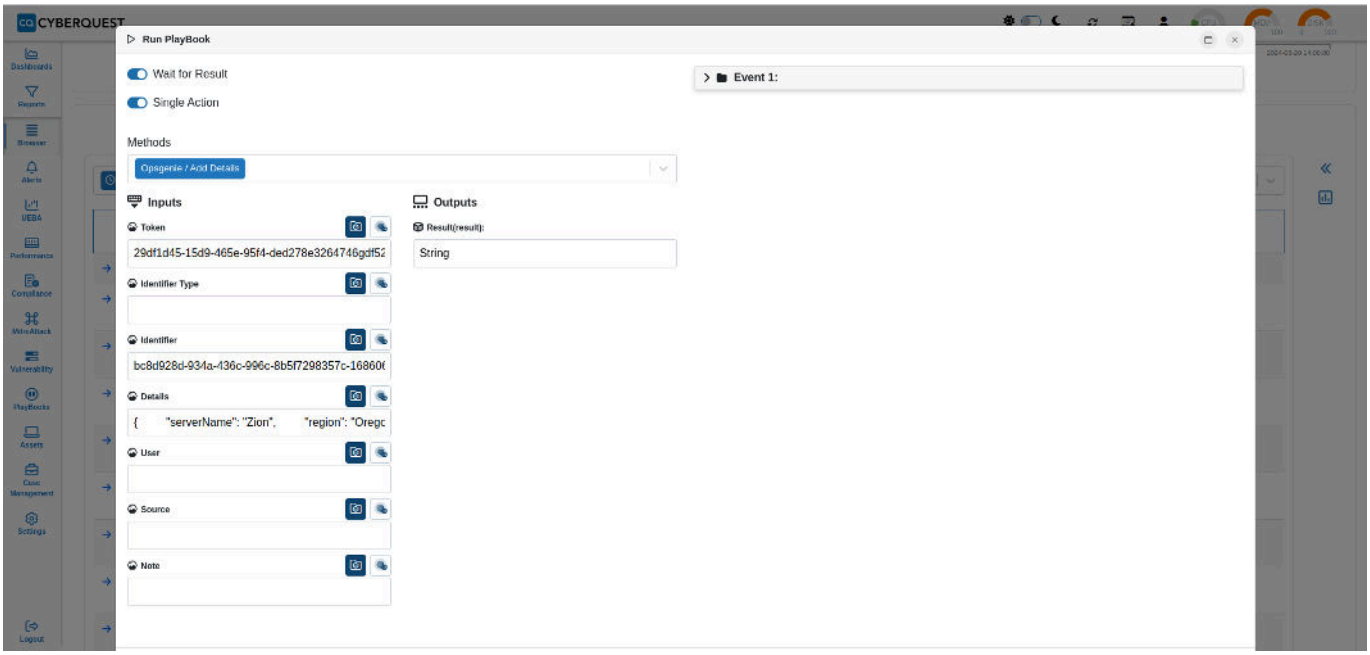


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Identifier Type	Type of the identifier that is provided as an in-line parameter. Possible values are id and name. Default value is id.
Identifier (is required)	Identifier of the alert
Tags (is required)	Comma separated list of tags to remove from alert.
Note	Additional alert note to add.

Outputs	Description
Result (result)	The result of the API call

Opsgenie/Add Details method

Add details to the alert with given identifier.

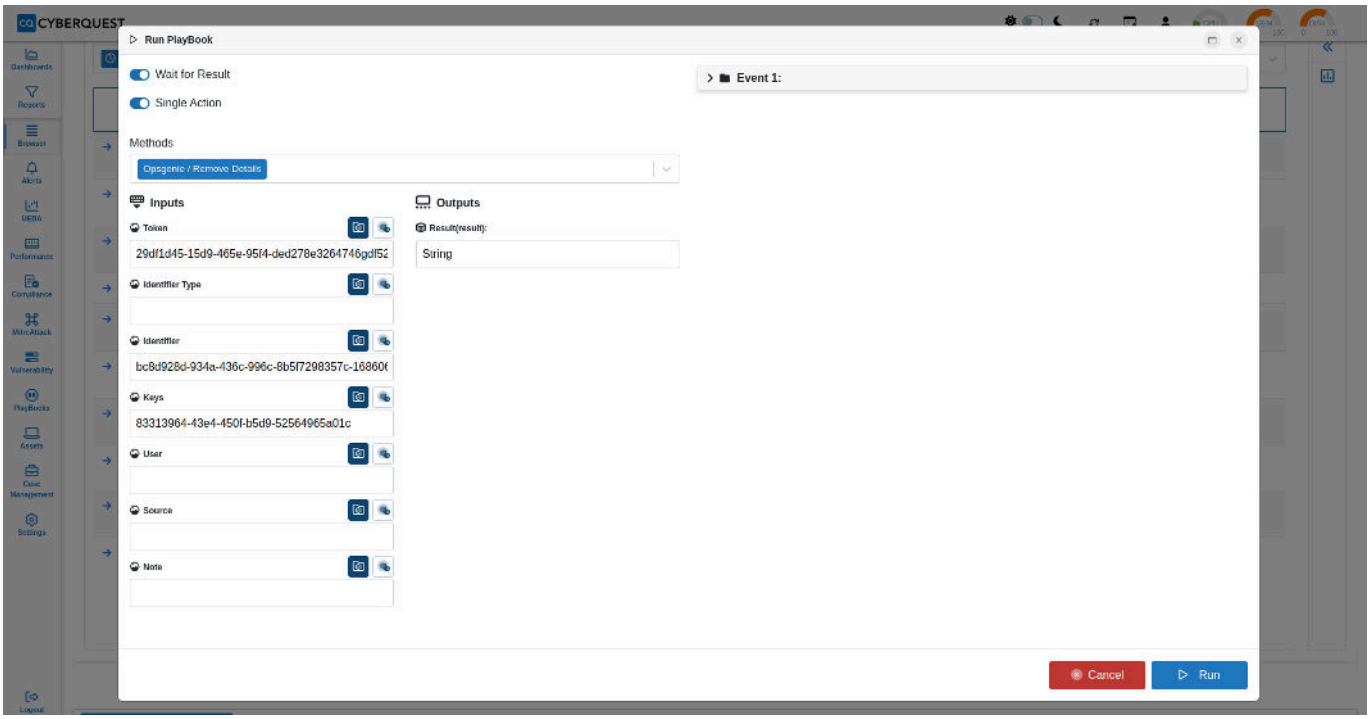


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Identifier Type	Type of the identifier that is provided as an in-line parameter. Possible values are id and name. Default value is id.
Identifier (is required)	Identifier of the alert
Details (is required)	Key-value pairs to add as custom property into alert. You can refer below for example values
User	Display name of the request owner.
Source	Display name of the request source.
Note	Additional alert note to add.

Outputs	Description
Result (result)	The result of the API call

Opsgenie/Remove Details method

Remove details of the alert with given identifier.

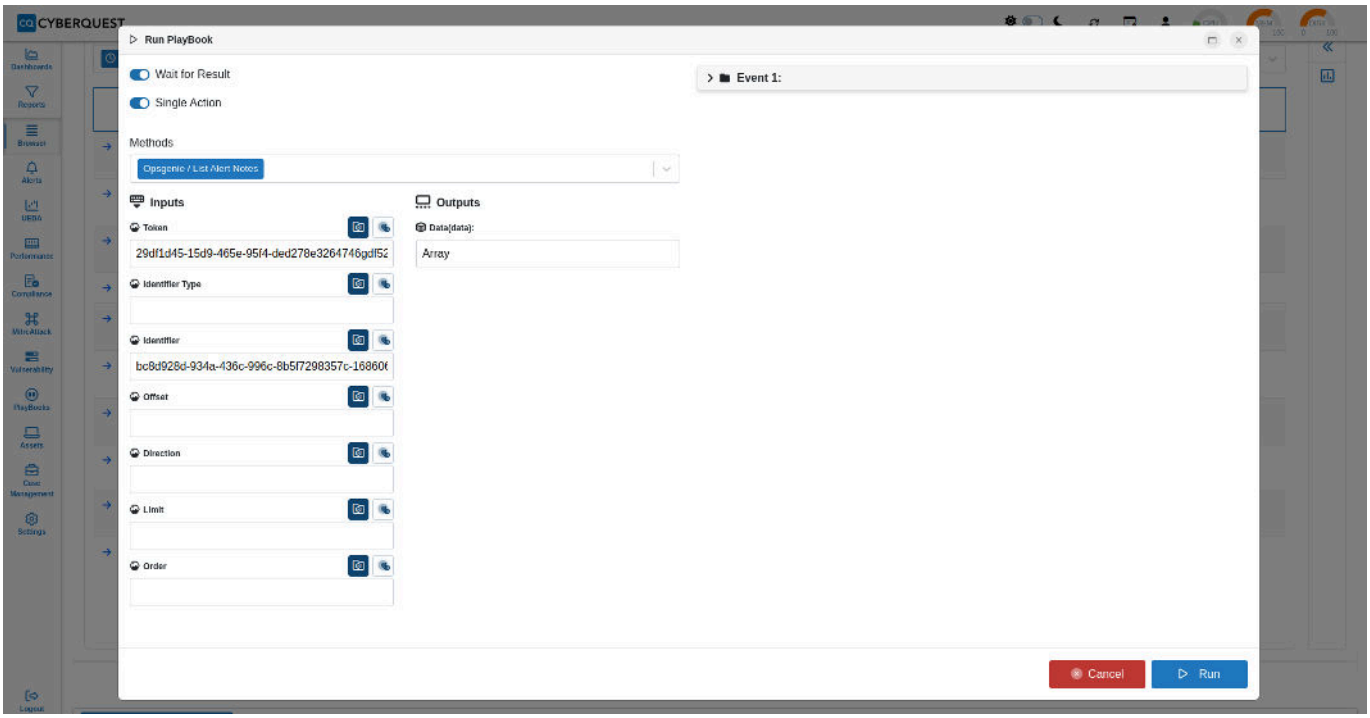


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Identifier Type	Type of the identifier that is provided as an in-line parameter. Possible values are id and name. Default value is id.
Identifier (is required)	Identifier of the alert
Keys (is required)	Comma separated list of keys to remove from the custom properties of the alert.
User	Display name of the request owner
Source	Display name of the request source.
Note	Additional alert note to add.

Outputs	Description
Result (result)	The result of the API call

Opsgenie/List Alert Notes method

List alert notes for the given alert identifier.

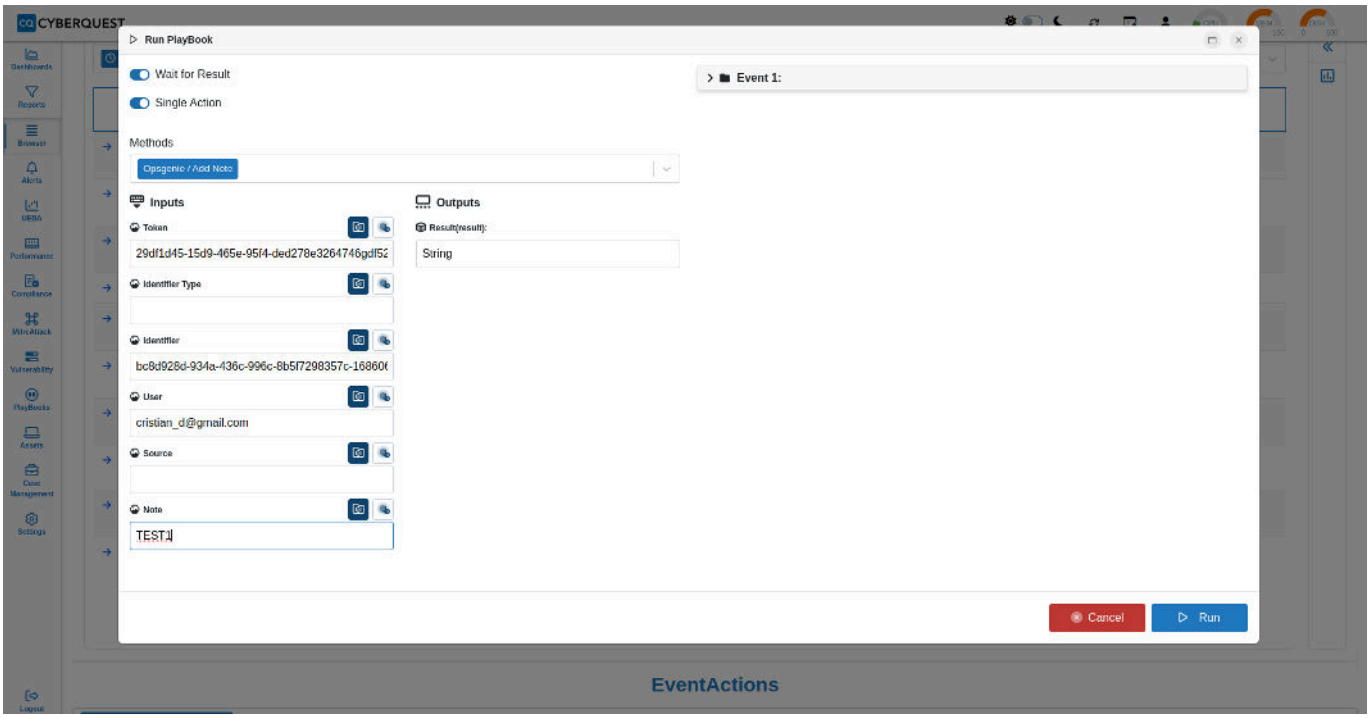


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Identifier Type	Type of the identifier that is provided as an in-line parameter. Possible values are id and name. Default value is id.
Identifier (is required)	Identifier of the alert
Offset	Starting value of the offset property
Direction	Page direction to apply for the given offset. Possible values are next and prev. Default value is next.next: Offset values of provided notes should be greater than the given offsetprev: Offset values of provided notes should be less than the given offset
Limit	Maximum number of items to provide in the result. Must be a positive integer value. Default value is 20 and maximum value is 100.
Order	Sorting order of the result set. Possible values are desc and asc. Default value is desc.desc: Sort result set in descending orderasc: Sort result set in ascending order

Outputs	Description
Data (data)	The result of the API call

Opsgenie/Add Note method

Adds note to alert with given identifier.

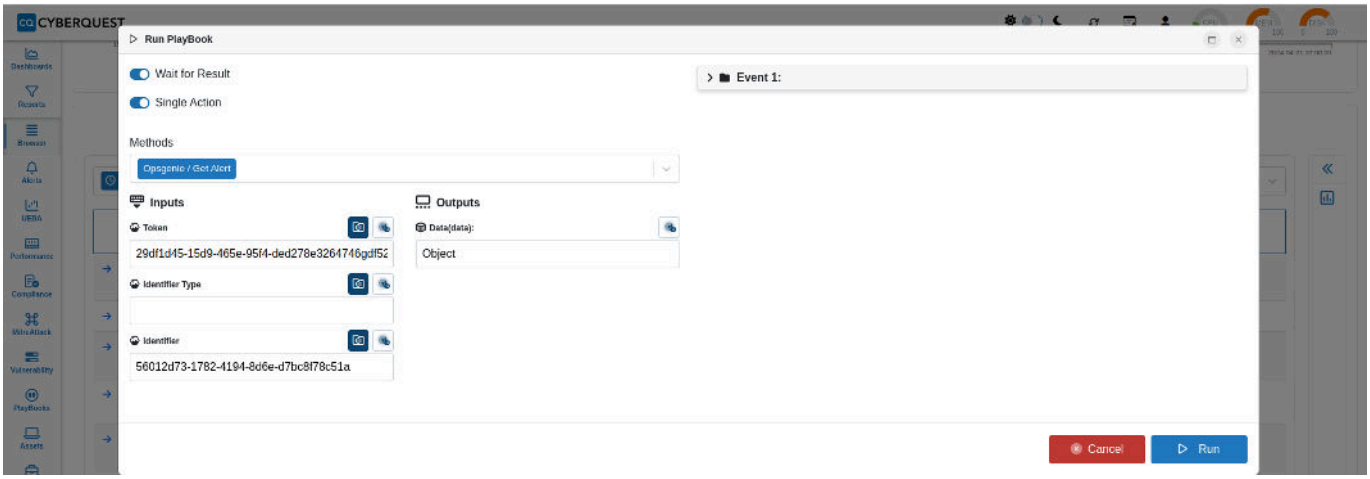


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Identifier Type	Type of the identifier that is provided as an in-line parameter. Possible values are id and name. Default value is id.
Identifier (is required)	Identifier of the alert
User	Display name of the request owner.
Source	Display name of the request source.
Note (is required)	Alert note to add

Outputs	Description
Result (result)	The result of the API call

Opsgenie/Get Alert method

Returns alert with given id, tiny id or alias.

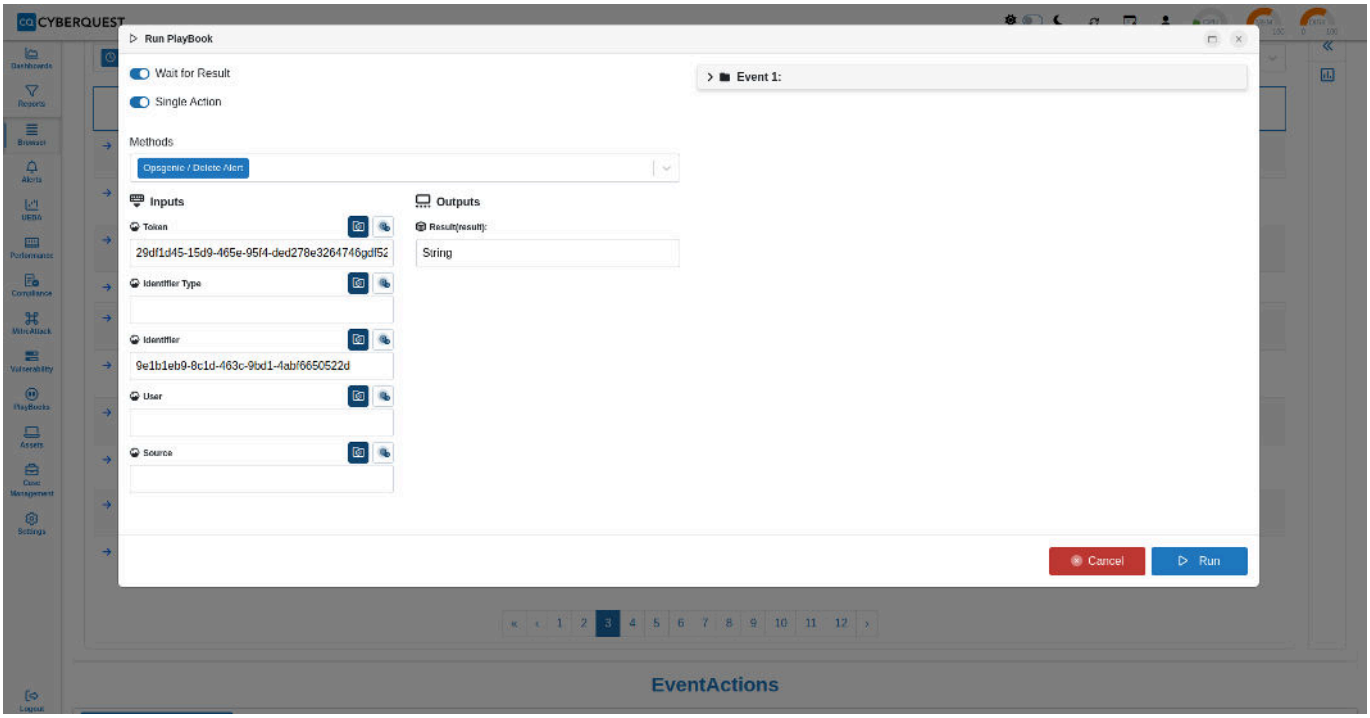


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Identifier Type	Type of the identifier that is provided as an in-line parameter. Possible values are id and name. Default value is id.
Identifier (is required)	Identifier of the alert

Outputs	Description
Data (data)	Details about the alert

Opsgenie/Delete Alert method

Deletes an alert using alert id, tiny id or alias.

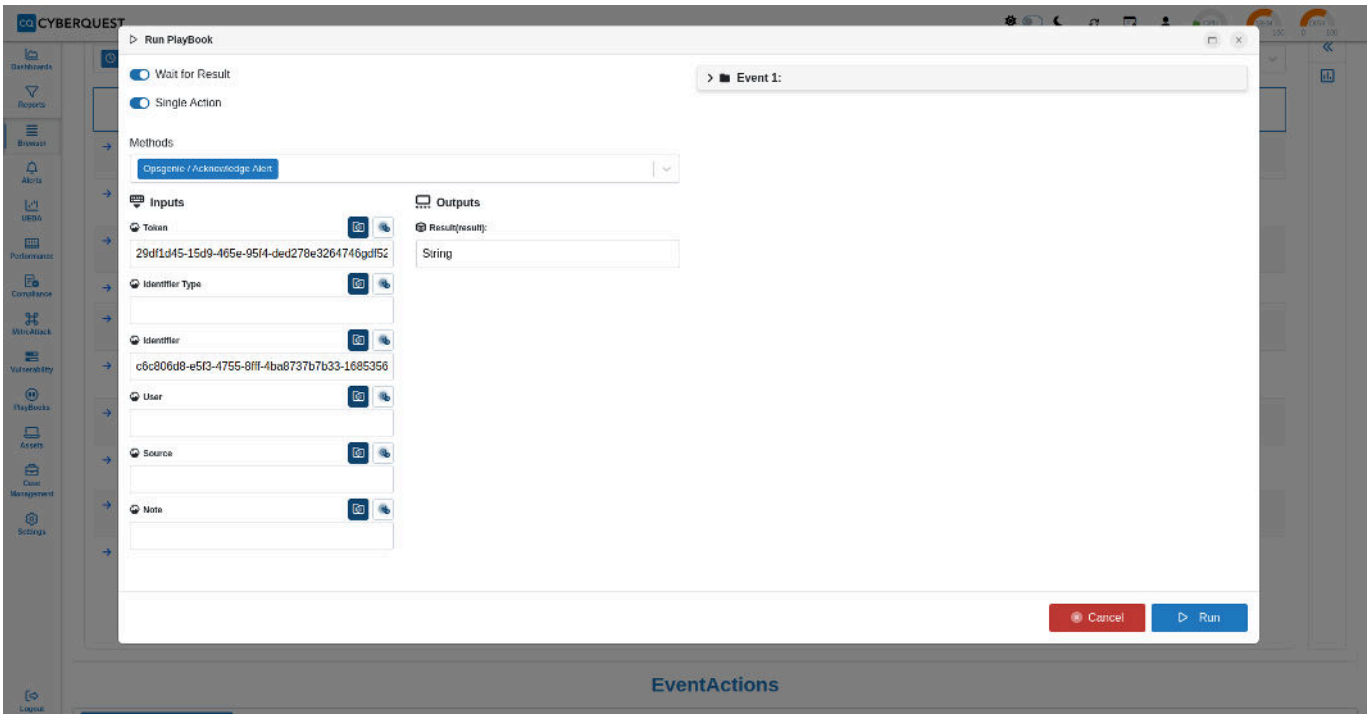


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Identifier Type	Type of the identifier that is provided as an in-line parameter. Possible values are id and name. Default value is id.
Identifier (is required)	Identifier of the alert
User	Display name of the request owner.
Source	Display name of the request source.

Outputs	Description
Result (result)	The result of the API call

Opsgenie/Acknowledge Alert method

Acknowledges alert with given identifier.

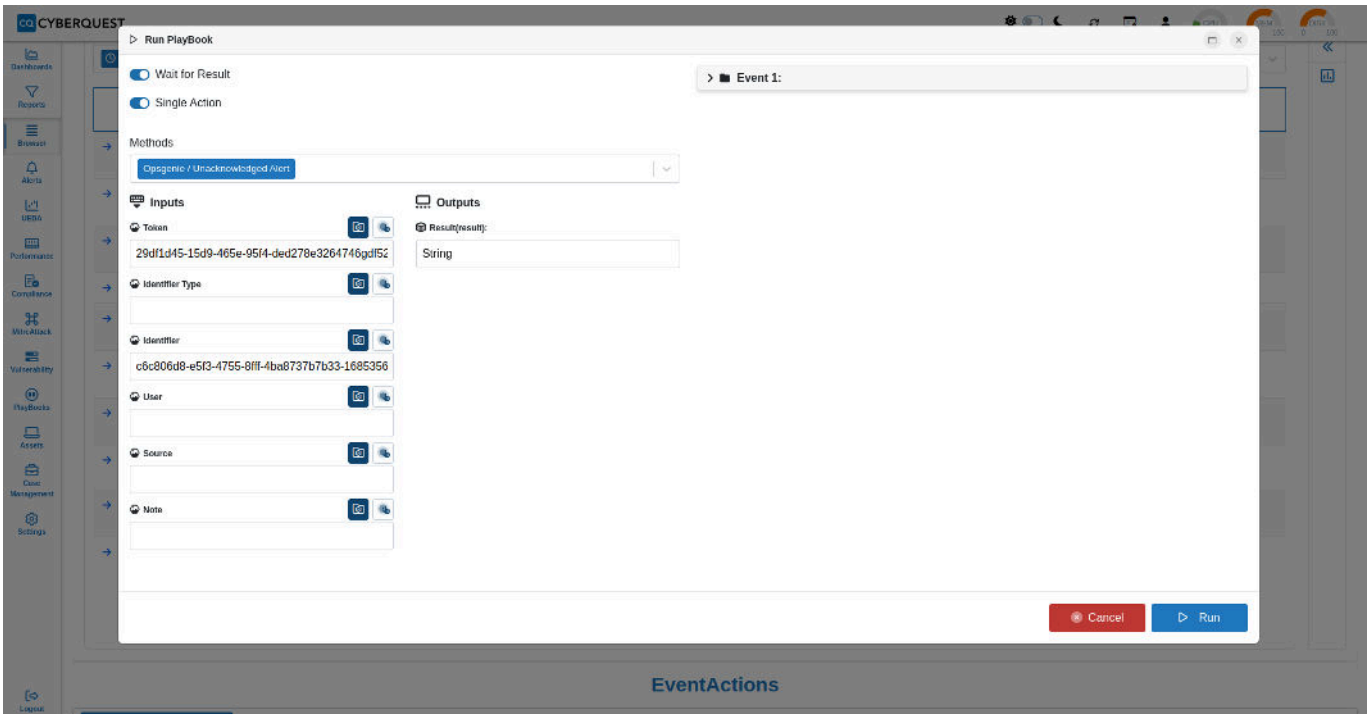


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Identifier Type	Type of the identifier that is provided as an in-line parameter. Possible values are id and name. Default value is id.
Identifier (is required)	Identifier of the alert
User	Display name of the request owner.
Source	Display name of the request source.
Note	Additional alert note to add

Outputs	Description
Result (result)	The result of the API call

Opsgenie/Unacknowledged Alert method

Unacknowledged alert with given identifier.

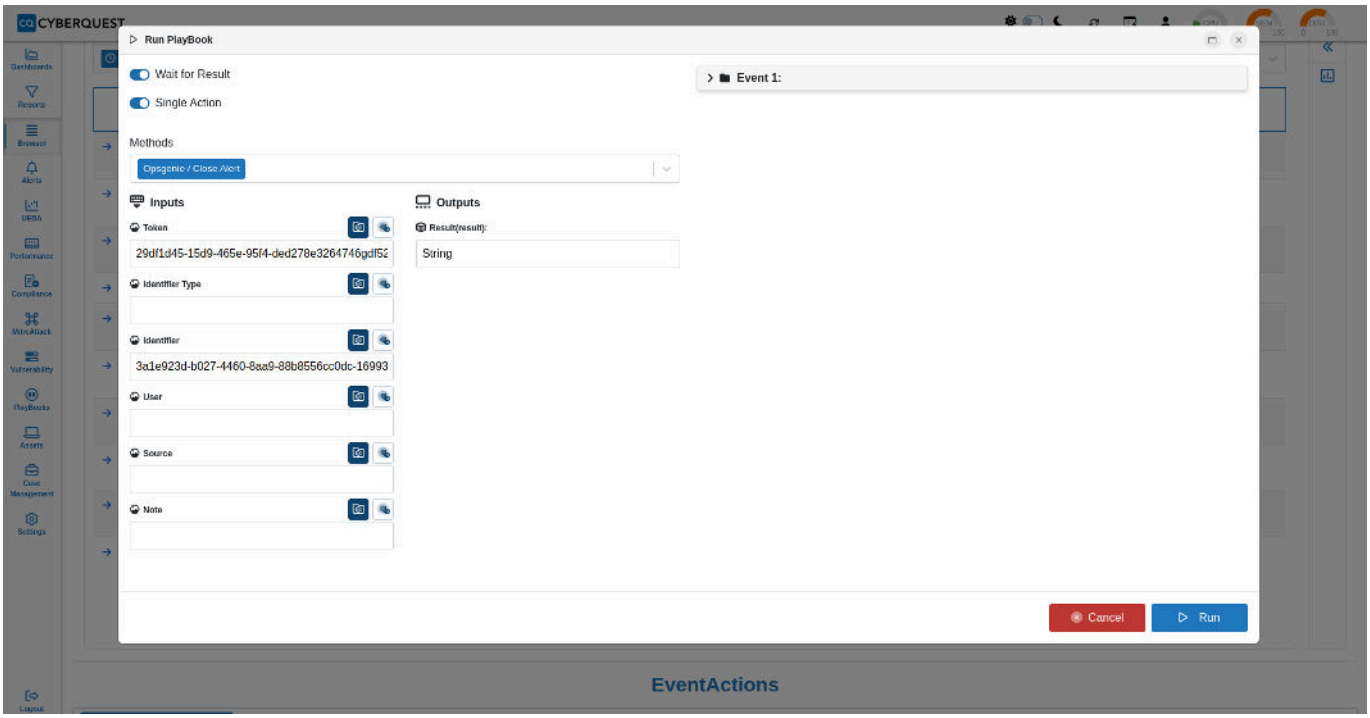


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Identifier Type	Type of the identifier that is provided as an in-line parameter. Possible values are id and name. Default value is id.
Identifier (is required)	Identifier of the alert
User	Display name of the request owner.
Source	Display name of the request source.
Note	Additional alert note to add

Outputs	Description
Result (result)	The result of the API call

Opsgenie/Close Alert method

Closes alert with given identifier.

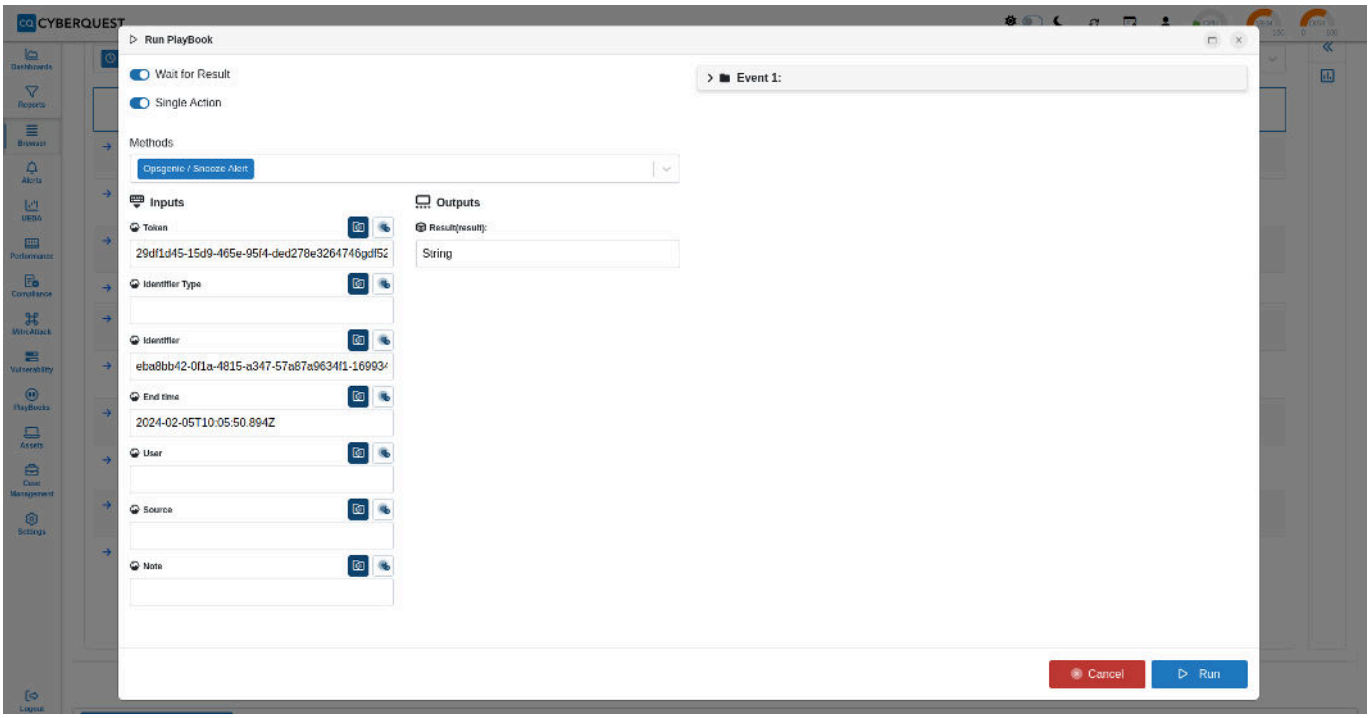


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Identifier Type	Type of the identifier that is provided as an in-line parameter. Possible values are id and name. Default value is id.
Identifier (is required)	Identifier of the alert
User	Display name of the request owner.
Source	Display name of the request source.
Note	Additional alert note to add

Outputs	Description
Result (result)	The result of the API call

Opsgenie/Snooze Alert method

Snooze alert with given identifier.

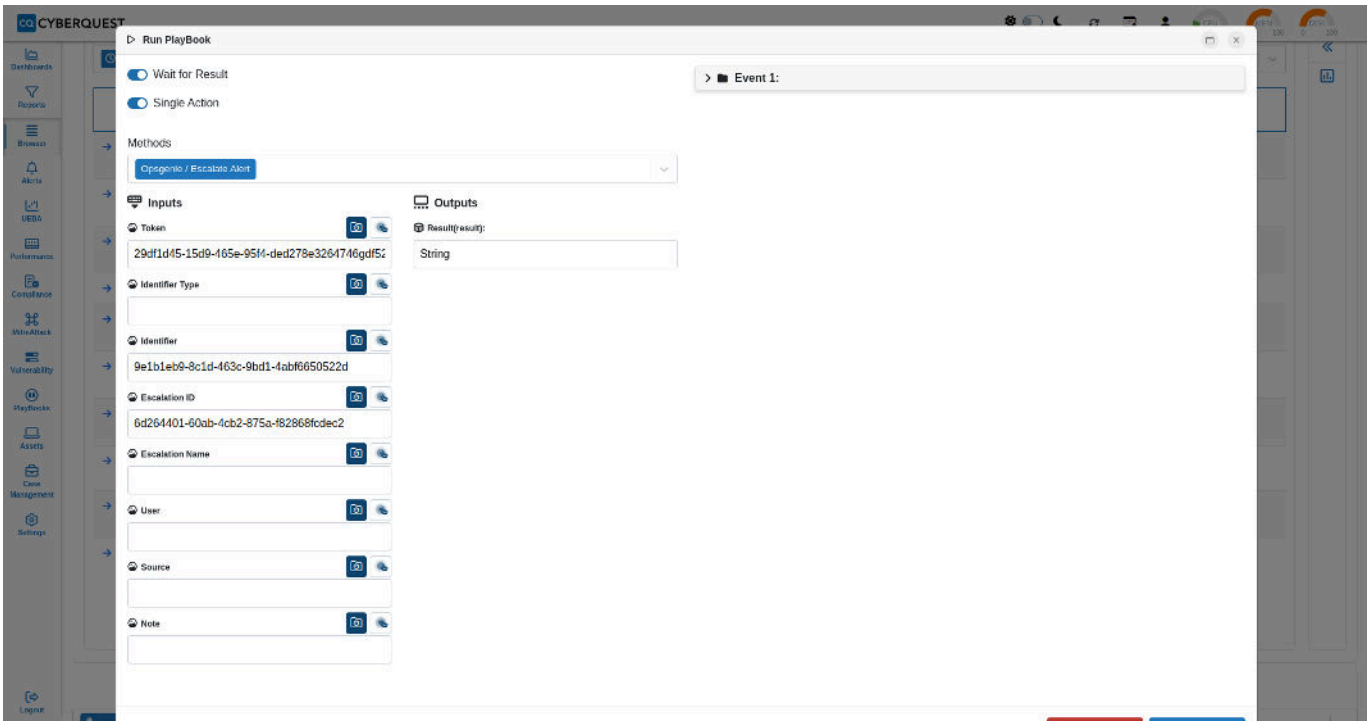


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Identifier Type	Type of the identifier that is provided as an in-line parameter. Possible values are id and name. Default value is id.
Identifier (is required)	Identifier of the alert
End time (is required)	Date and time that snooze will lose effect. Provided value should be in ISO 8061 format.
User	Display name of the request owner.
Source	Display name of the request source.
Note	Additional alert note to add

Outputs	Description
Result (result)	The result of the API call

Opsgenie/Escalate Alert method

Escalate alert with given identifier.

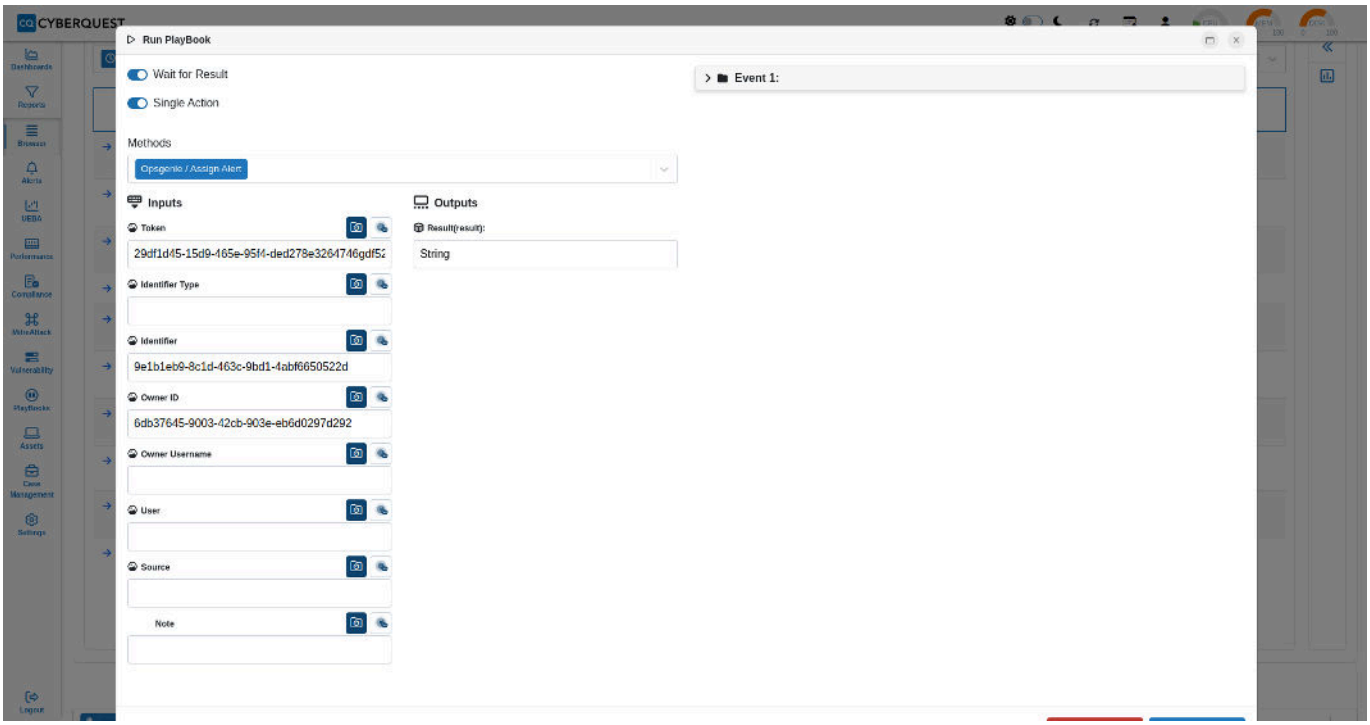


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Identifier Type	Type of the identifier that is provided as an in-line parameter. Possible values are id and name. Default value is id.
Identifier (is required)	Identifier of the alert
Escalation ID	Escalation that the alert will be escalated. Escalation ID or Escalation Name is required to work
Escalation Name	Escalation that the alert will be escalated. Escalation ID or Escalation Name is required to work
User	Display name of the request owner.
Source	Display name of the request source.
Note	Additional alert note to add

Outputs	Description
Result (result)	The result of the API call

Opsgenie/Assign Alert method

Assign alert with given identifier.

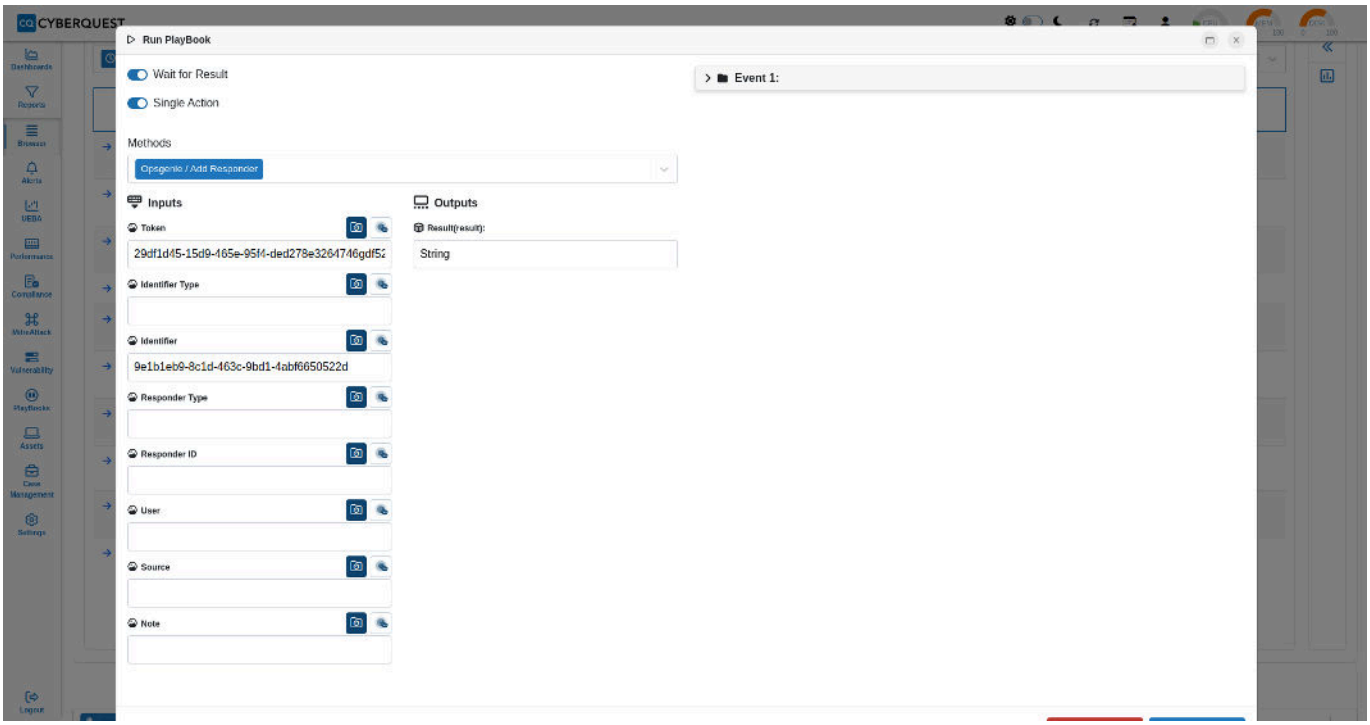


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Identifier Type	Type of the identifier that is provided as an in-line parameter. Possible values are id and name. Default value is id.
Identifier (is required)	Identifier of the alert
Owner ID	User that the alert will be assigned to. Either id or username of the user should be provided. You can refer below for example values.
Owner Username	User that the alert will be assigned to. Either id or username of the user should be provided. You can refer below for example values.
User	Display name of the request owner.
Source	Display name of the request source.
Note	Identifier of the saved search

Outputs	Description
Result (result)	The result of the API call

Opsgenie/Add Responder method

Add responder to alert with given identifier.

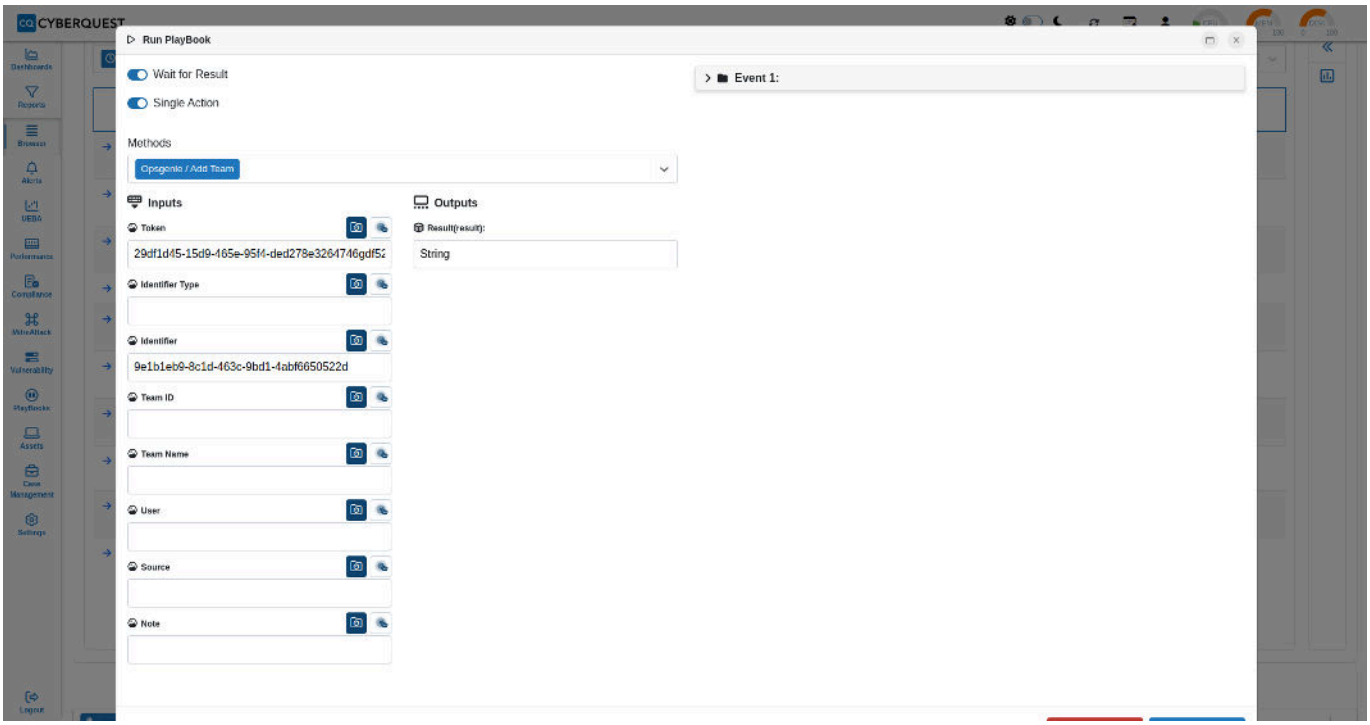


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Identifier Type	Type of the identifier that is provided as an in-line parameter. Possible values are id and name. Default value is id.
Identifier (is required)	Identifier of the alert
Responder Type	Team or user that the alert will be routed to. type field is mandatory for item, where possible values are team and user. In addition to the type field id should be given. You can refer below for example values.
Responder ID	Team or user that the alert will be routed to. type field is mandatory for item, where possible values are team and user. In addition to the type field id should be given. You can refer below for example values.
User	Display name of the request owner.
Source	Display name of the request source.
Note	Additional alert note to add

Outputs	Description
Result (result)	The result of the API call

Opsgenie/Add Team method

Add team to alert with given identifier.

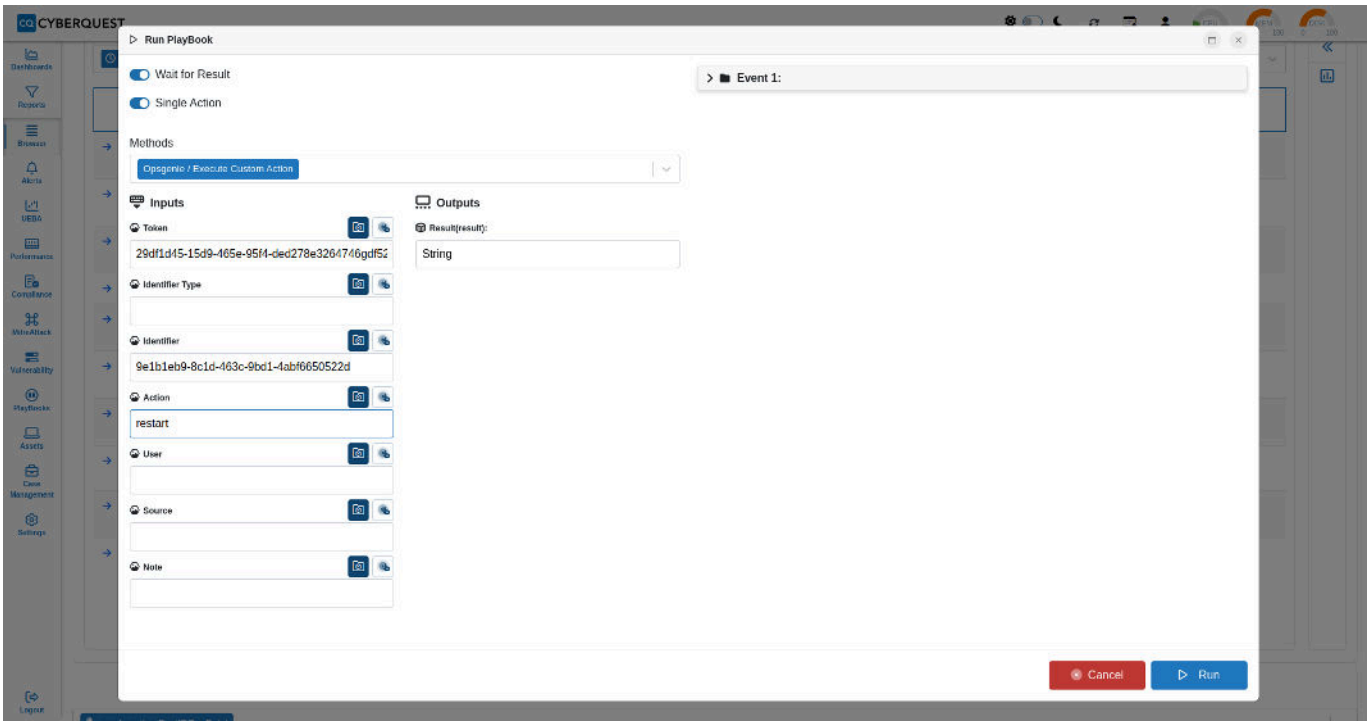


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Identifier Type	Type of the identifier that is provided as an in-line parameter. Possible values are id and name. Default value is id.
Identifier (is required)	Identifier of the alert
Team ID	Team or user that the alert will be routed to. type field is mandatory for item, where possible values are team and user. In addition to the type field id should be given. You can refer below for example values.
Team Name	Team or user that the alert will be routed to. type field is mandatory for item, where possible values are team and user. In addition to the type field id should be given. You can refer below for example values.
User	Display name of the request owner.
Source	Display name of the request source.
Note	Additional alert note to add

Outputs	Description
Result (result)	The result of the API call

Opsgenie/Execute Custom Action method

Custom actions for the alert.

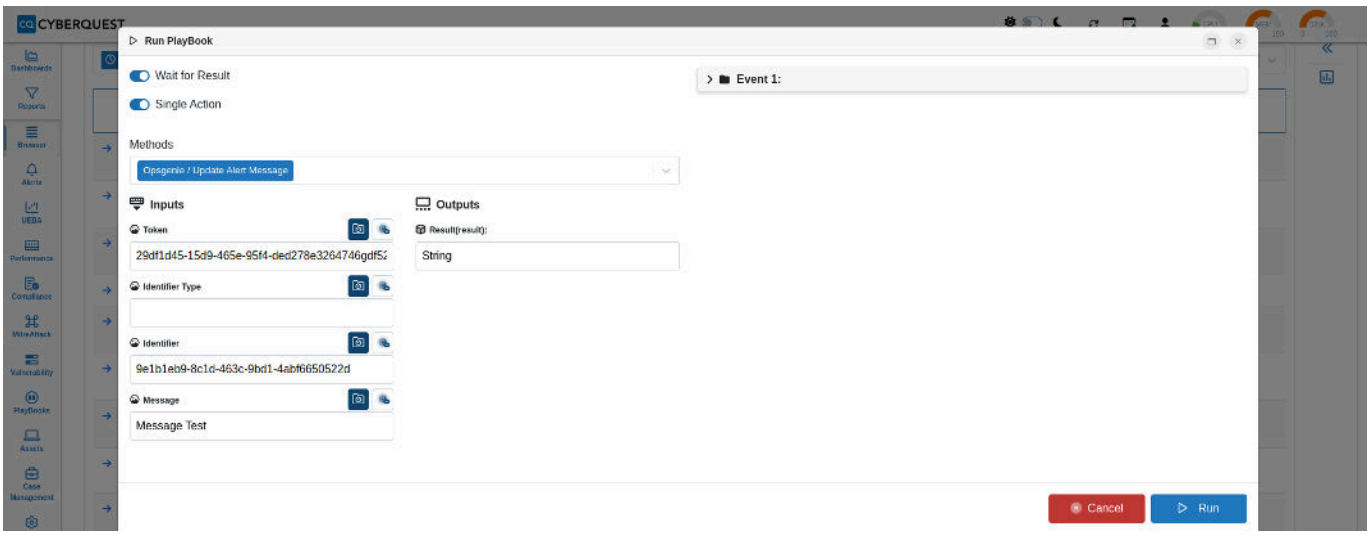


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Identifier Type	Type of the identifier that is provided as an in-line parameter. Possible values are id and name. Default value is id.
Identifier (is required)	Identifier of the alert
Action (is required)	Name of the action to execute
User	Display name of the request owner.
Source	Display name of the request source.
Note	Additional alert note to add

Outputs	Description
Result (result)	The result of the API call

Opsgenie/Update Alert Message method

Update the message of the alert with given identifier.

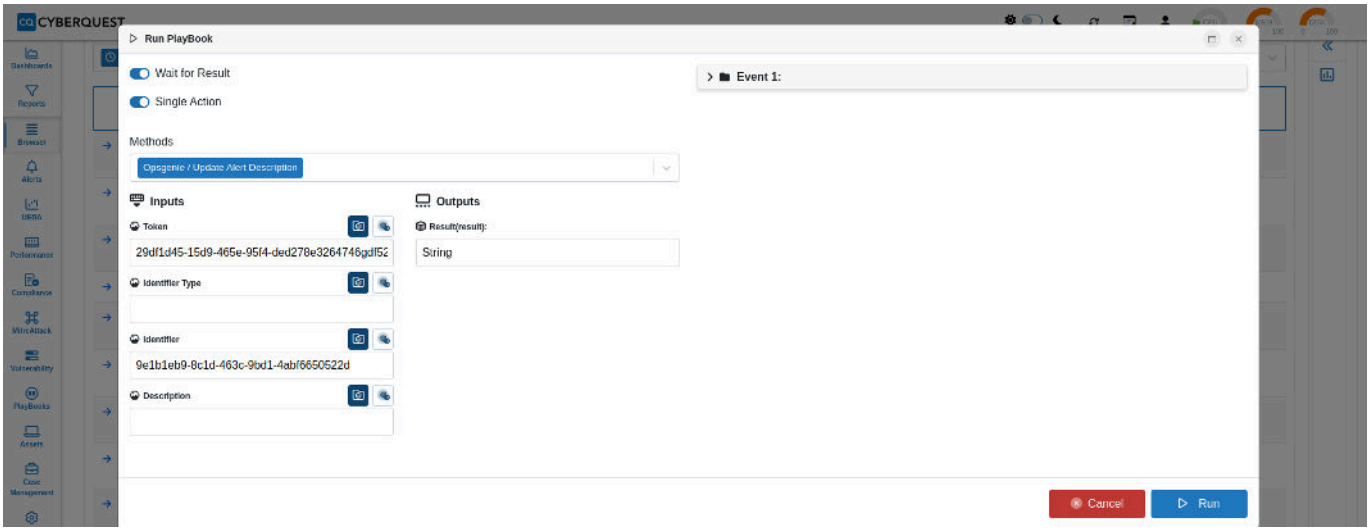


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Identifier Type	Type of the identifier that is provided as an in-line parameter. Possible values are id and name. Default value is id.
Identifier (is required)	Identifier of the alert
Message (is required)	Message of the alert.

Outputs	Description
Result (result)	The result of the API call

Opsgenie/Update Alert Description method

Update the description of the alert with given identifier.

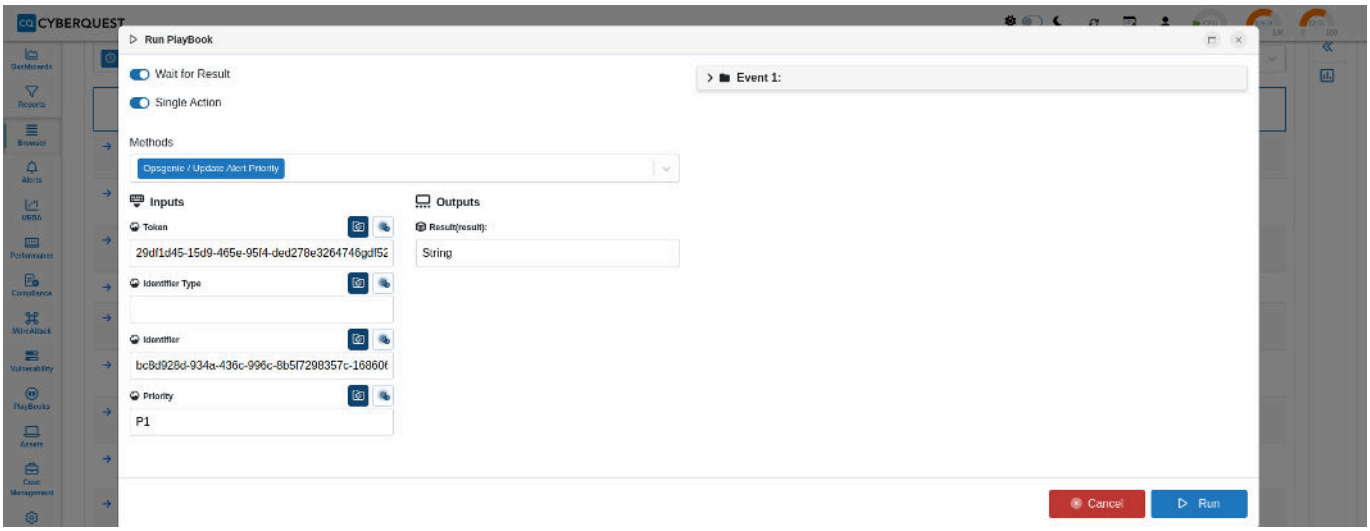


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Identifier Type	Type of the identifier that is provided as an in-line parameter. Possible values are id and name. Default value is id.
Identifier (is required)	Identifier of the alert
Description	Description of the alert.

Outputs	Description
Result (result)	The result of the API call

Opsgenie/Update Alert Priority method

Update the priority of the alert with given identifier.

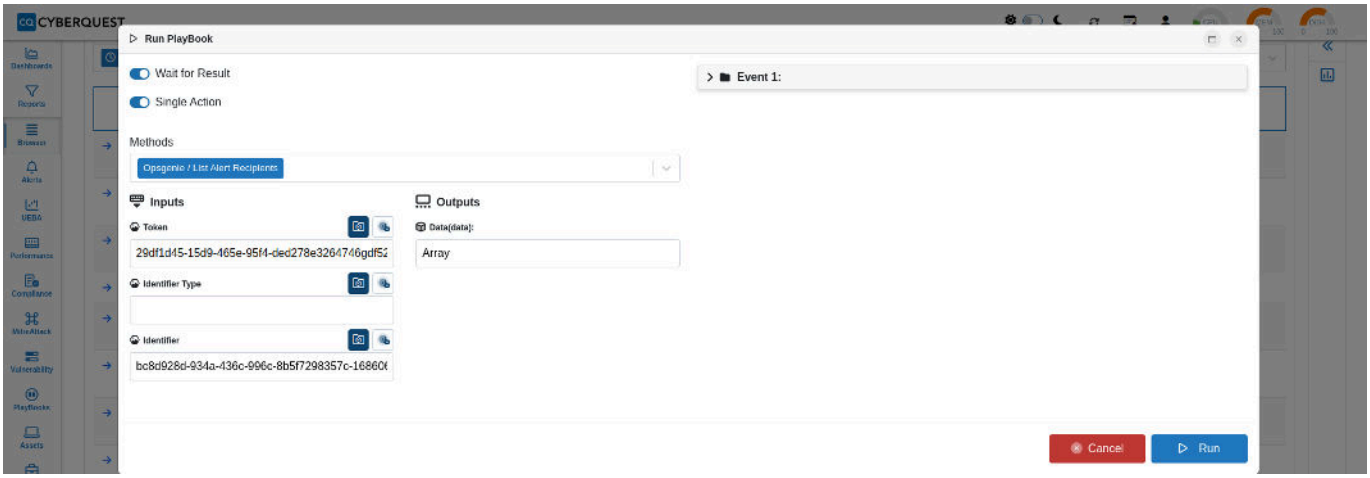


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Identifier Type	Type of the identifier that is provided as an in-line parameter. Possible values are id and name. Default value is id.
Identifier (is required)	Identifier of the alert
Priority (is required)	Description of the alert.

Outputs	Description
Result (result)	The result of the API call

Opsgenie/List Alert Recipients method

List alert recipients for the given alert identifier.

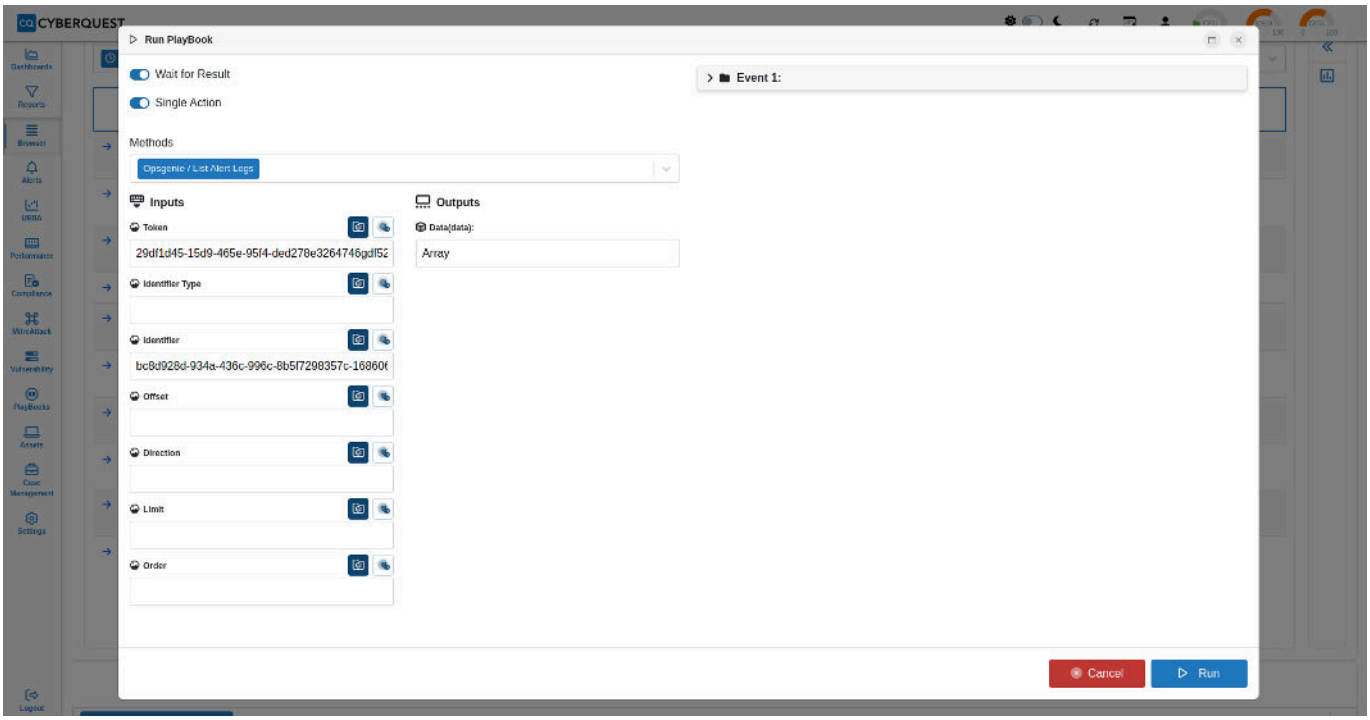


Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Identifier Type	Type of the identifier that is provided as an in-line parameter. Possible values are id and name. Default value is id.
Identifier (is required)	Identifier of the alert

Outputs	Description
Data (data)	The result of the API call

Opsgenie/List Alert Logs method

List alert logs for the given alert identifier.



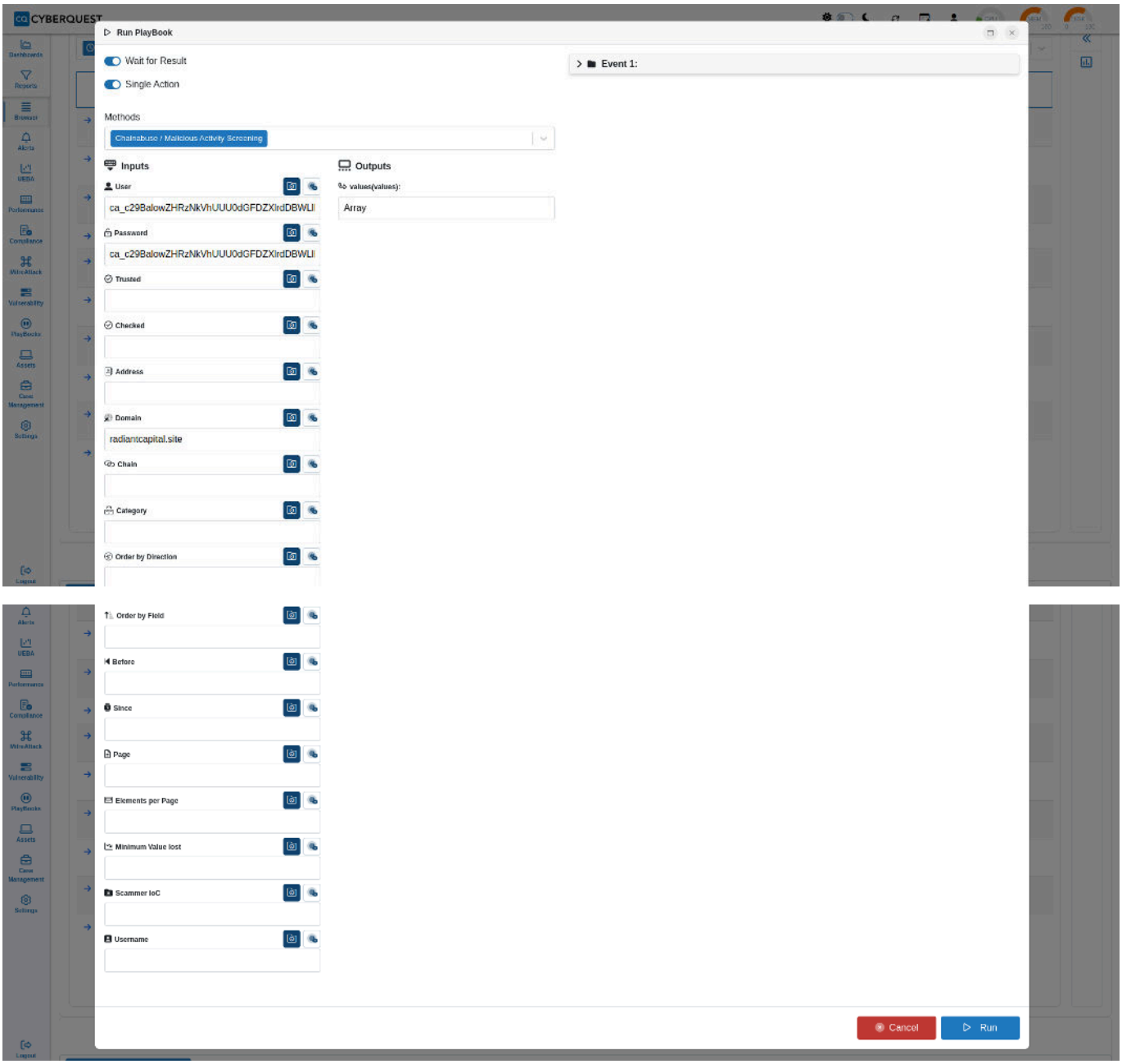
Inputs	Description
Token (is required)	To use the Opsgenie API, you must have an API key.
Identifier Type	Type of the identifier that is provided as an in-line parameter. Possible values are id and name. Default value is id.
Identifier (is required)	Identifier of the alert
Offset	Starting value of the offset property.
Direction	Page direction to apply for the given offset. Possible values are next and prev. Default value is next.next: Offset values of provided logs should be greater than the given offsetprev: Offset values of provided logs should be less than the given offset
Limit	Maximum number of items to provide in the result. Must be a positive integer value. Default value is 20 and maximum value is 100.
Order	Sorting order of the result set. Possible values are desc and asc. Default value is desc.desc: Sort result set in descending orderasc: Sort result set in ascending order

Outputs	Description
Data (data)	The result of the API call

Chainabuse

Chainabuse/Malicious Activity Screening method

This API allows users to screen addresses and URLs to verify whether they have been reported as linked to malicious activity on Chainabuse.

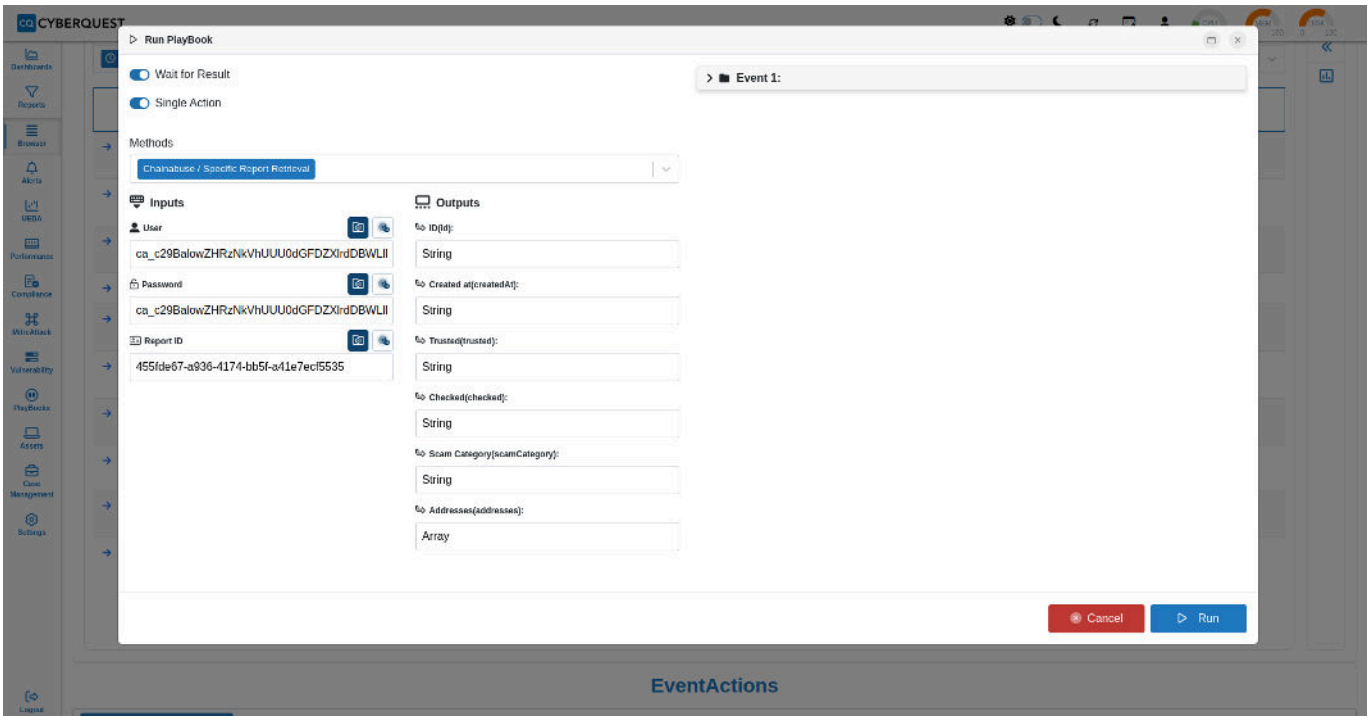

CYBERQUEST
Run PlayBook
Wait for Result
Single Action
Methods
Chainabuse / Malicious Activity Screening
Inputs
Outputs
User
ca_c29BalowZHRzNkVhUUU0dGFDZXlrdDBWLl
values(values):
Array
Password
ca_c29BalowZHRzNkVhUUU0dGFDZXlrdDBWLl
Trusted
Checked
Address
Domain
radiantcapital.site
Chain
Category
Order by Direction
Order by Field
Before
Since
Page
Elements per Page
Minimum Value lost
Scammer IoC
Username
Event 1:
Cancel
Run

Inputs	Description
User (is required)	Introduce Api key here
Password (is required)	Introduce Api key here
Trusted	True: reported by a trusted contributor, based on how this Partner detects and verifies information.False: the reporter is not registered as a trusted contributor. Please note this does not mean their report cannot be trusted.
Checked	True: report checked by our team of moderators including blockchain intelligence experts.False: report could not be verified by our team of moderators.
Address	(Optional if a domain is passed). Crypto addresses to screen.
Domain	(Optional if an address is passed). URL to screen.
Chain	(Optional if a URL is passed). Chain to use as filter.
Category	Optional. Scam category to use as filter.
Order by Direction	ASC = latest reports firstDESC= oldest report first if several reports are pulled out
Order by Field	Orders reports by date if several reports are pulled out
Before	Optional. Threshold date to use as a filter.
Since	Optional. Start date to use as a filter.
Page	Optional. Number of pages of reports to pull out. The maximum number of reports per page is 50. If page =1, you will pull out a maximum of 50 reports.
Elements per Page	Optional. Number of reports to display per page. The maximum number of reports per page is 50. If page =1, you will pull out a maximum of 50 reports.
Minimum Value lost	Optional. Filters reports with at least the amount passed (Currently, only usd asset are supported and others will be ignored).
Scammer IoC	Optional. Filters reports based on passed indicator of compromise.
Username	Optional. The contributors username.

Outputs	Description
values (values)	The results of the API call

Chainabuse/Specific Report Retrieval method

This API allows users to retrieve a specific report using its ID.



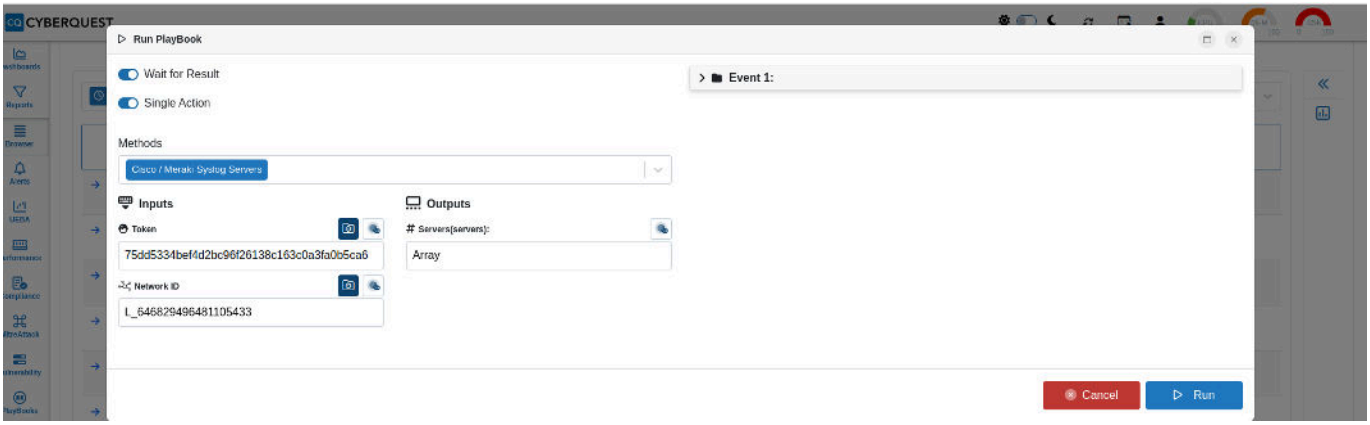
Inputs	Description
User (is required)	Introduce API key here
Password (is required)	Introduce Api key here
Report ID (is required)	Id of the report

Outputs	Description
ID (id)	The ID of the report
Created at (createdAt)	The date when the report was created
Trusted (trusted)	Reported by a contributor registered as trusted on Chainabuse
Checked (checked)	If the raport was verified
Scam Category (scamCategory)	The category of the scam where the report was classified
Addresses (addresses)	The addresses involved in scam

Cisco

Cisco/Meraki Syslog Servers method

List the syslog servers for a network.

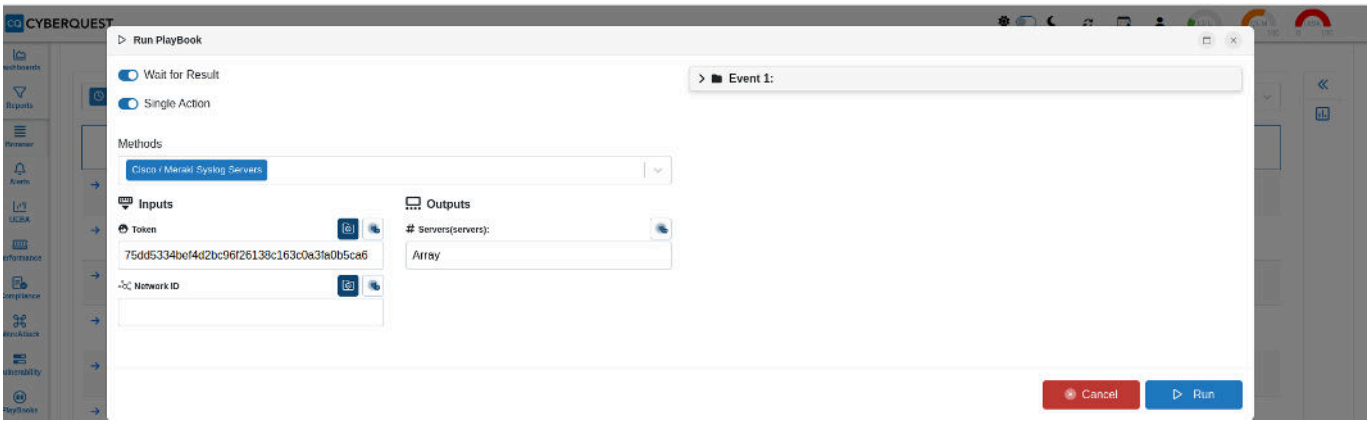


Inputs	Description
Token (is required)	To use the Cisco API, you must have an API key.
Network ID	The ID of the investigated network

Outputs	Description
Servers (servers)	A list of Syslog servers

Cisco/Meraki Traffic Analysis method

Return the traffic analysis settings for a network.

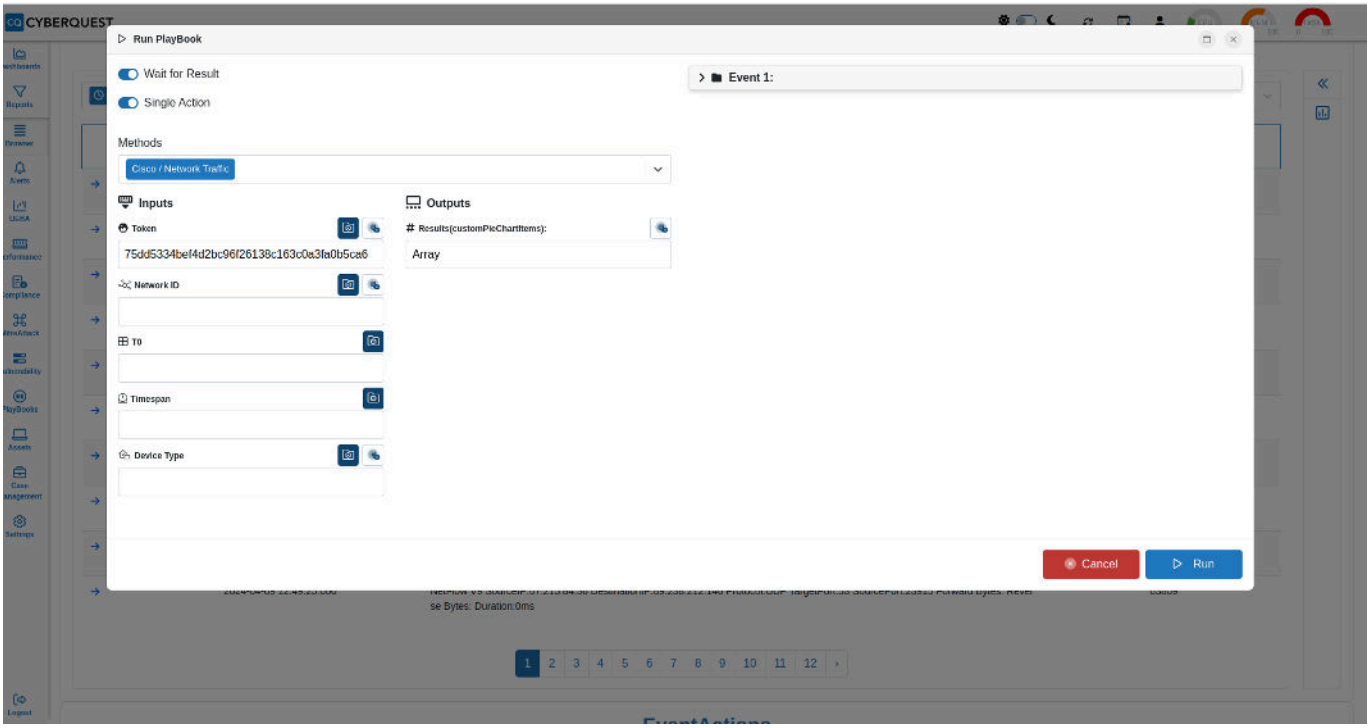


Inputs	Description
Token (is required)	To use the Cisco API, you must have an API key.
Network ID	The ID of the investigated network

Outputs	Description
Mode (mode)	The traffic analysis mode for the network. Can be one of 'disabled' (do not collect traffic types),'basic' (collect generic traffic categories), or 'detailed' (collect destination hostnames)
Results (customPieChartItems)	The list of items that make up the custom pie chart for traffic reporting.

Cisco/Network Traffic method

Return the traffic analysis data for this network. Traffic analysis with hostname visibility must be enabled on the network.

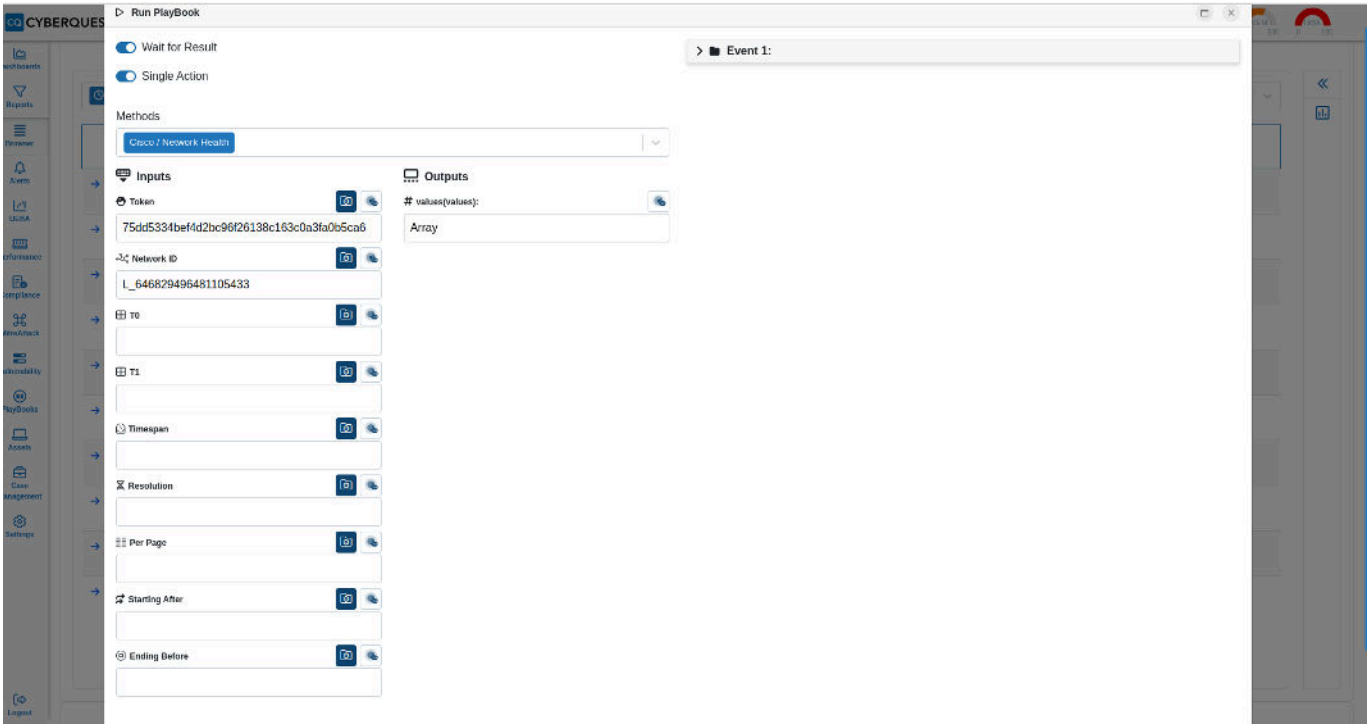


Inputs	Description
Token (is required)	To use the Cisco API, you must have an API key
Network ID	The ID of the investigated network
T0	
Timespan	
Device Type	Filter the data by device type: combined, wireless, switch or appliance. Defaults to combined. When using combined, for each rule the data will come from the device type with the most usage

Outputs	Description
Results (customPieChartItems)	The list of items that make up the custom pie chart for traffic reporting

Cisco/Network Health method

Get the channel utilization over each radio for all APs in a network.

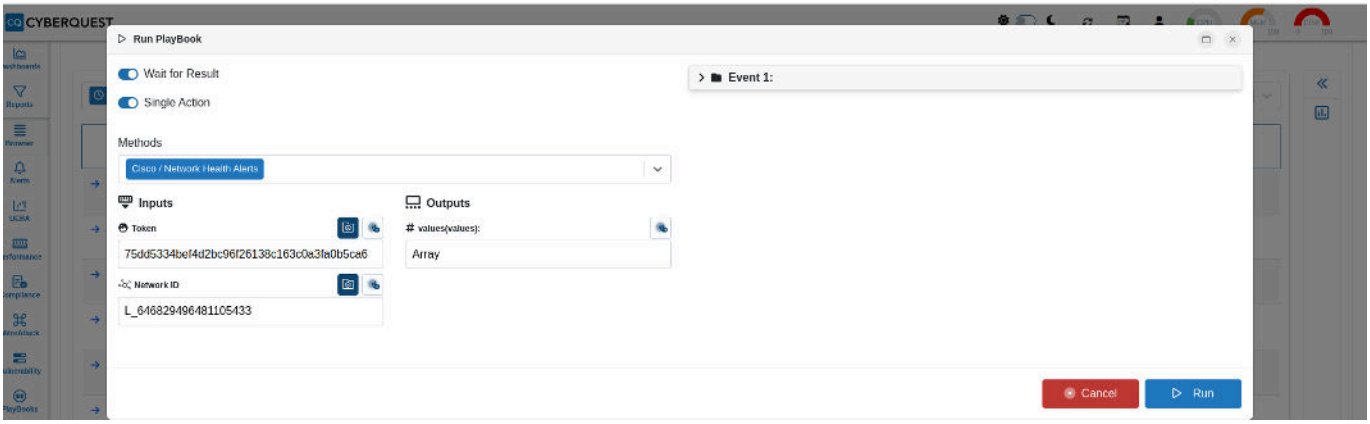


Inputs	Description
Token (is required)	To use the Cisco API, you must have an API key
Network ID (is required)	The ID of the investigated network
T0	The beginning of the timespan for the data. The maximum lookback period is 31 days from today
T1	The end of the timespan for the data. t1 can be a maximum of 31 days after t0
Timespan	The timespan for which the information will be fetched. If specifying timespan, do not specify parameters t0 and t1. The value must be in seconds and be less than or equal to 31 days. The default is 1 day
Resolution	The time resolution in seconds for returned data. The valid resolutions are: 600. The default is 600
Per Page	The number of entries per page returned. Acceptable range is 3 - 100. Default is 10
Starting After	A token used by the server to indicate the start of the page. Often this is a timestamp or an ID but it is not limited to those. This parameter should not be defined by client applications. The link for the first, last, prev, or next page in the HTTP Link header should define it
Ending Before	A token used by the server to indicate the end of the page. Often this is a timestamp or an ID but it is not limited to those. This parameter should not be defined by client applications. The link for the first, last, prev, or next page in the HTTP Link header should define it

Outputs	Description
values (values)	The results of the API call

Cisco/Network Health Alerts method

Return all global alerts on this network.

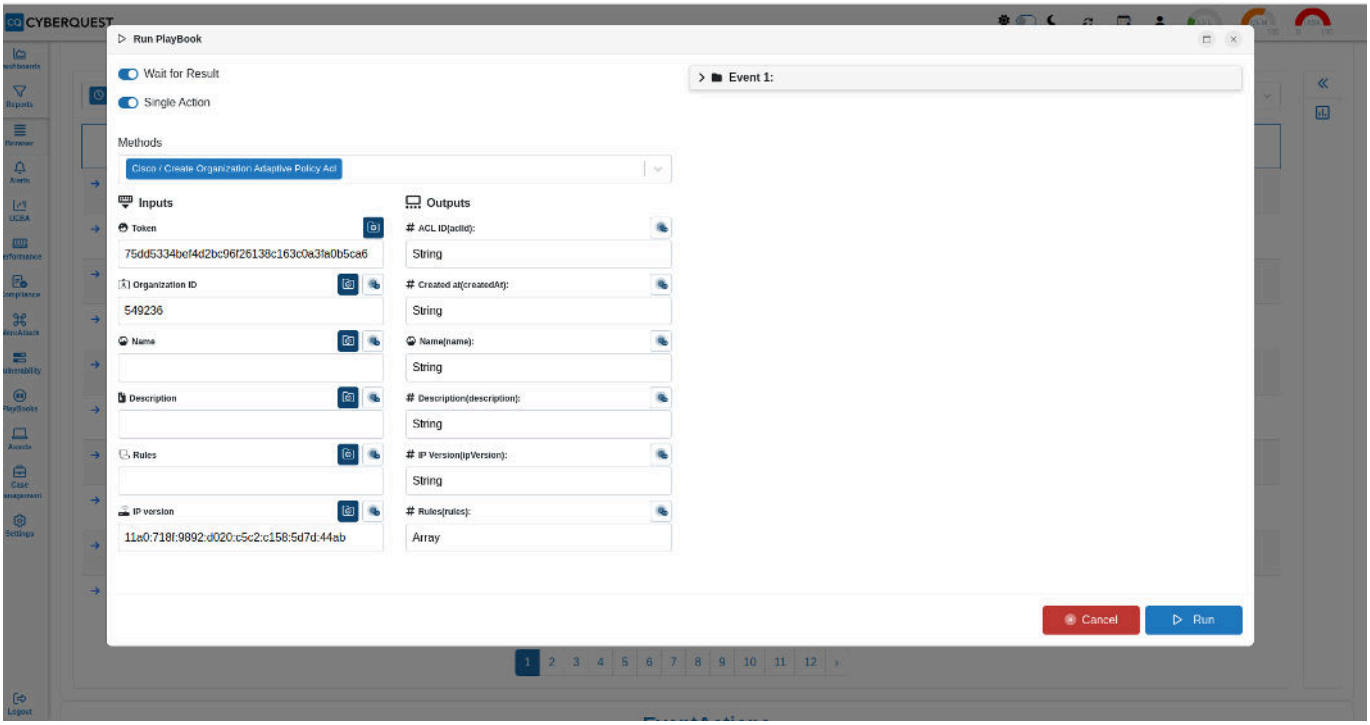


Inputs	Description
Token (is required)	To use the Cisco API, you must have an API key.
Network ID (is required)	The ID of the investigated network

Outputs	Description
values (values)	The results of the API call

Cisco/Create Organization Adaptive Policy Acl method

Creates new adaptive policy ACL.

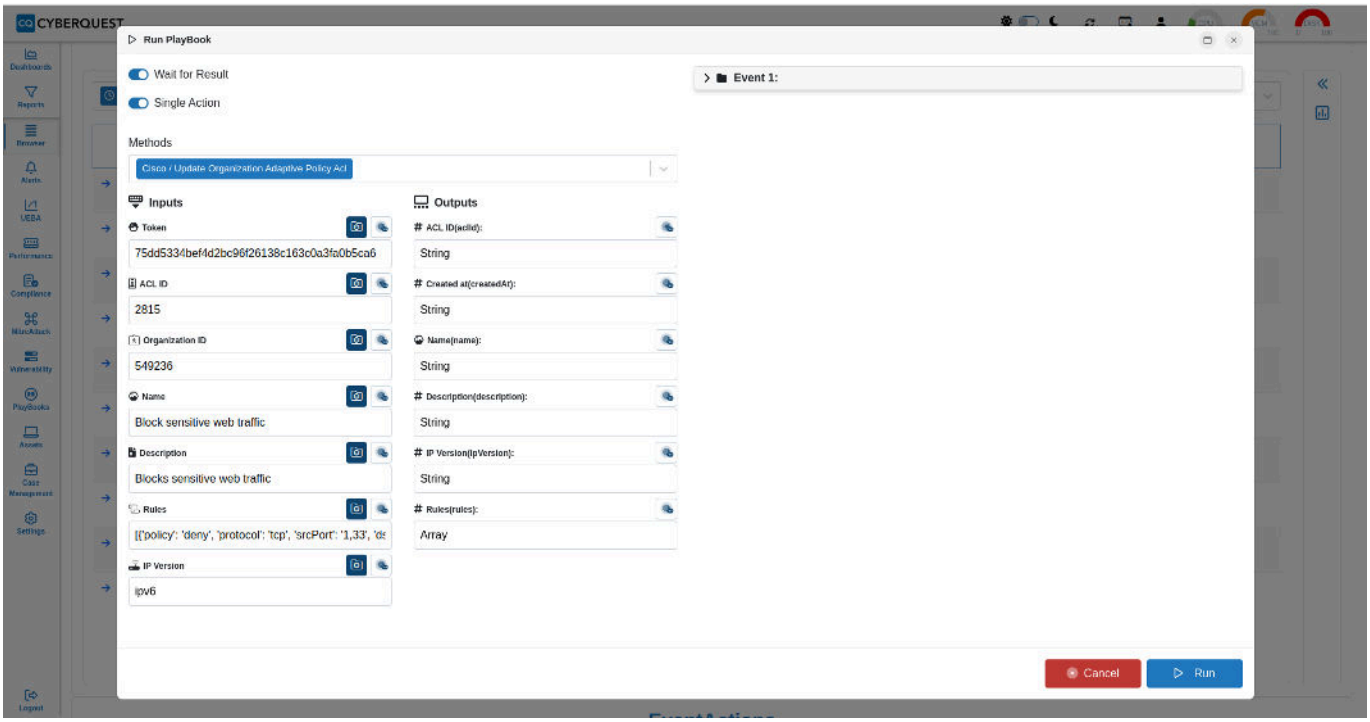


Inputs	Description
Token (is required)	
Organization ID (is required)	The ID of the Organization
Name	Name of the adaptive policy ACL
Description	Description of the adaptive policy ACL
Rules	An ordered array of the adaptive policy ACL rules.
IP version (is required)	IP version of adaptive policy ACL. One of: any, ipv4 or ipv6

Outputs	Description
ACL ID (aclId)	ID of the adaptive policy ACL
Created at (createdAt)	When the adaptive policy ACL was created
Name (name)	Name of the adaptive policy ACL
Description (description)	Description of the adaptive policy ACL
IP Version (ipVersion)	IP version of adaptive policy ACL
Rules (rules)	An ordered array of the adaptive policy ACL rules

Cisco/Update Organization Adaptive Policy Acl method

Updates an adaptive policy ACL.

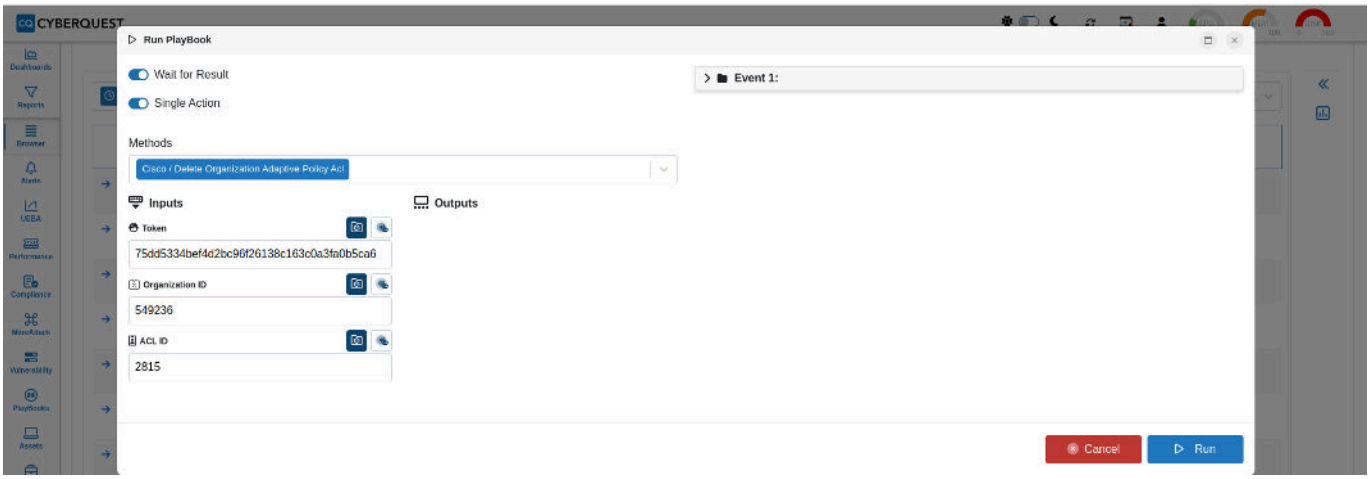


Inputs	Description
Token (is required)	To use the Cisco API, you must have an API key.
ACL ID (is required)	ID of the adaptive policy ACL
Organization ID (is required)	The ID of the Organization
Name (is required)	Name of the adaptive policy ACL
Description (is required)	Description of the adaptive policy ACL
Rules (is required)	An ordered array of the adaptive policy ACL rules. An empty array will clear the rules.
IP Version (is required)	IP version of adaptive policy ACL

Outputs	Description
ACL ID (aclId)	ID of the adaptive policy ACL
Created at (createdAt)	When the adaptive policy ACL was created
Name (name)	Name of the adaptive policy ACL
Description (description)	Description of the adaptive policy ACL
IP Version (ipVersion)	IP version of adaptive policy ACL
Rules (rules)	An ordered array of the adaptive policy ACL rules

Cisco/Delete Organization Adaptive Policy Acl method

Deletes the specified adaptive policy ACL. Note this adaptive policy ACL will also be removed from policies using it.

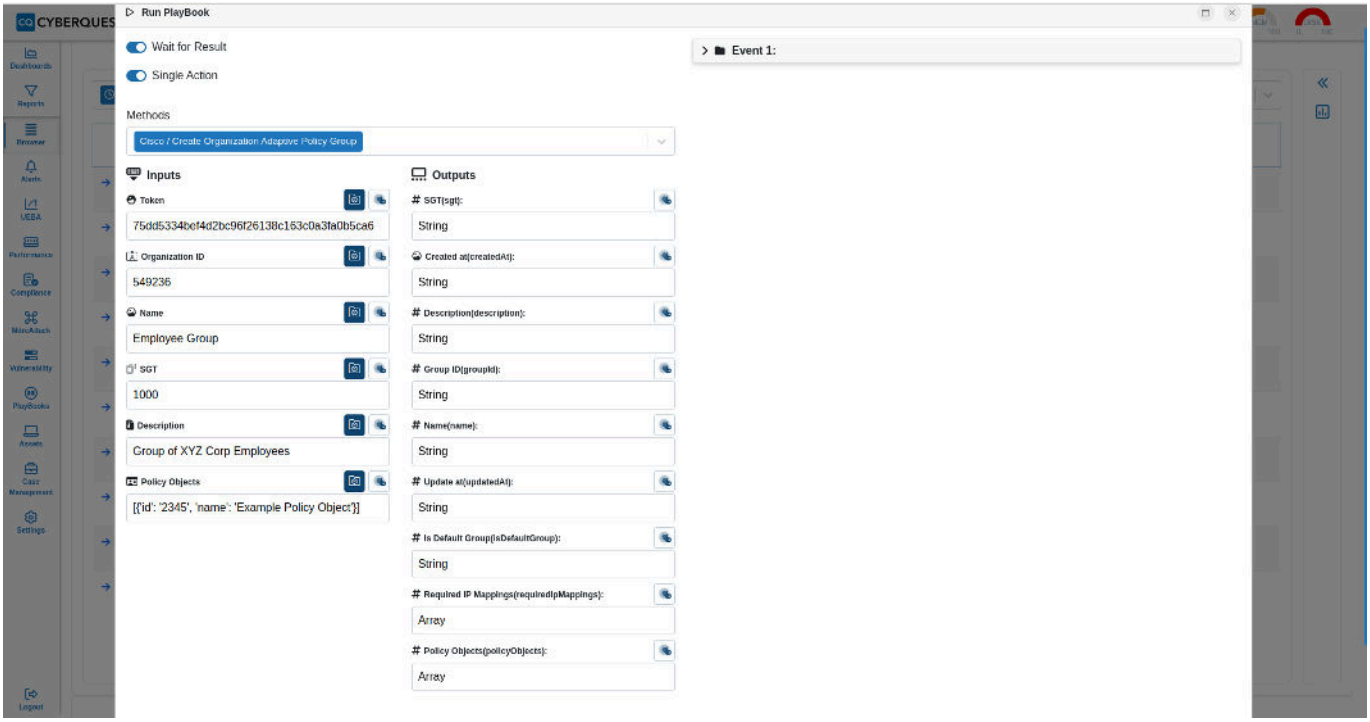


Inputs	Description
Token (is required)	To use the Cisco API, you must have an API key.
Organization ID (is required)	The ID of the Organization
ACL ID (is required)	ID of the adaptive policy ACL

Outputs	Description

Cisco/Create Organization Adaptive Policy Group method

Creates a new adaptive policy group.

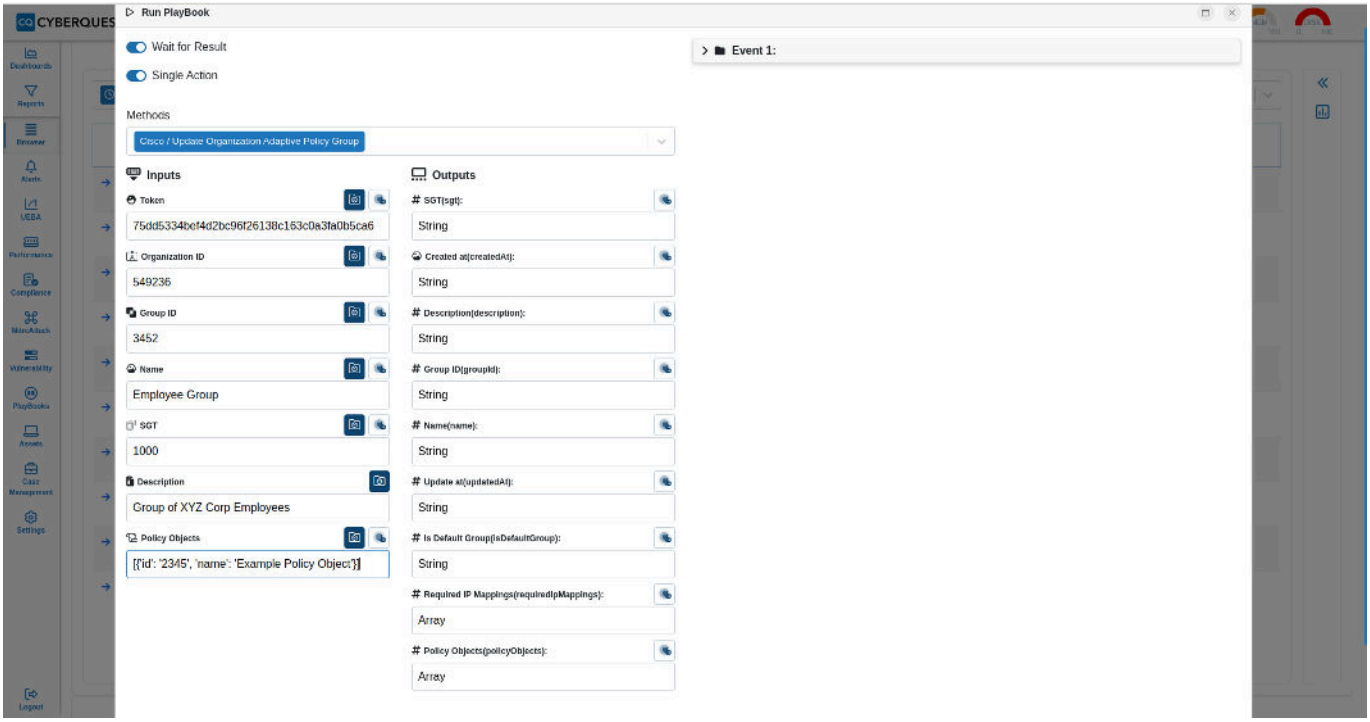


Inputs	Description
Token (is required)	To use the Cisco API, you must have an API key.
Organization ID (is required)	The ID of the Organization
Name (is required)	Name of the adaptive policy ACL
SGT (is required)	SGT value of the group
Description (is required)	Description of the group
Policy Objects (is required)	The ID of the policy object

Outputs	Description
SGT (sgt)	The security group tag for the adaptive policy group
Created at (createdAt)	Created at timestamp for the adaptive policy group
Description (description)	The description for the adaptive policy group
Group ID (groupId)	The ID of the adaptive policy group
Name (name)	The name of the adaptive policy group
Update at (updatedAt)	Updated at timestamp for the adaptive policy group
Is Default Group (isDefaultGroup)	Whether the adaptive policy group is the default group
Required IP Mappings (requiredIpMappings)	List of required IP mappings for the adaptive policy group
Policy Objects (policyObjects)	The policy objects for the adaptive policy group

Cisco/Update Organization Adaptive Policy Group method

Updates an adaptive policy group. If updating Infrastructure, only the SGT is allowed. Cannot update Unknown.

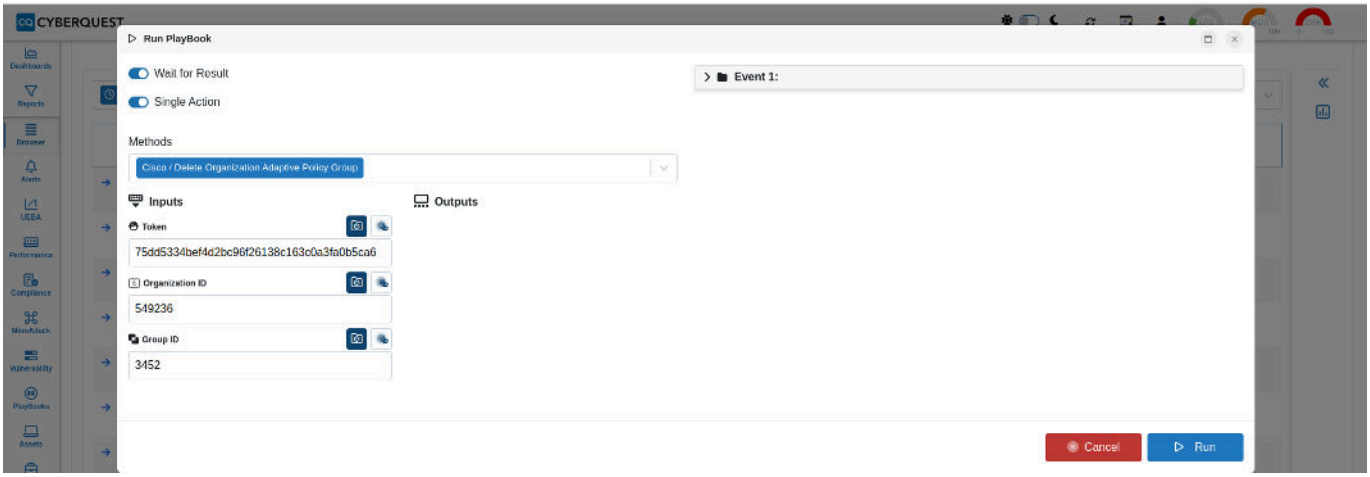


Inputs	Description
Token (is required)	To use the Cisco API, you must have an API key.
Organization ID (is required)	The ID of the Organization
Group ID (is required)	The ID of the adaptive policy group
Name (is required)	Name of the group
SGT (is required)	SGT value of the group
Description (is required)	
Policy Objects (is required)	The policy objects for the adaptive policy group

Outputs	Description
SGT (sgt)	The security group tag for the adaptive policy group
Created at (createdAt)	Created at timestamp for the adaptive policy group
Description (description)	The description for the adaptive policy group
Group ID (groupId)	The ID of the adaptive policy group
Name (name)	The name of the adaptive policy group
Update at (updatedAt)	Updated at timestamp for the adaptive policy group
Is Default Group (isDefaultGroup)	Whether the adaptive policy group is the default group
Required IP Mappings (requiredIpMappings)	List of required IP mappings for the adaptive policy group
Policy Objects (policyObjects)	The policy objects for the adaptive policy group

Cisco/Delete Organization Adaptive Policy Group method

Deletes the specified adaptive policy group and any associated policies and references.

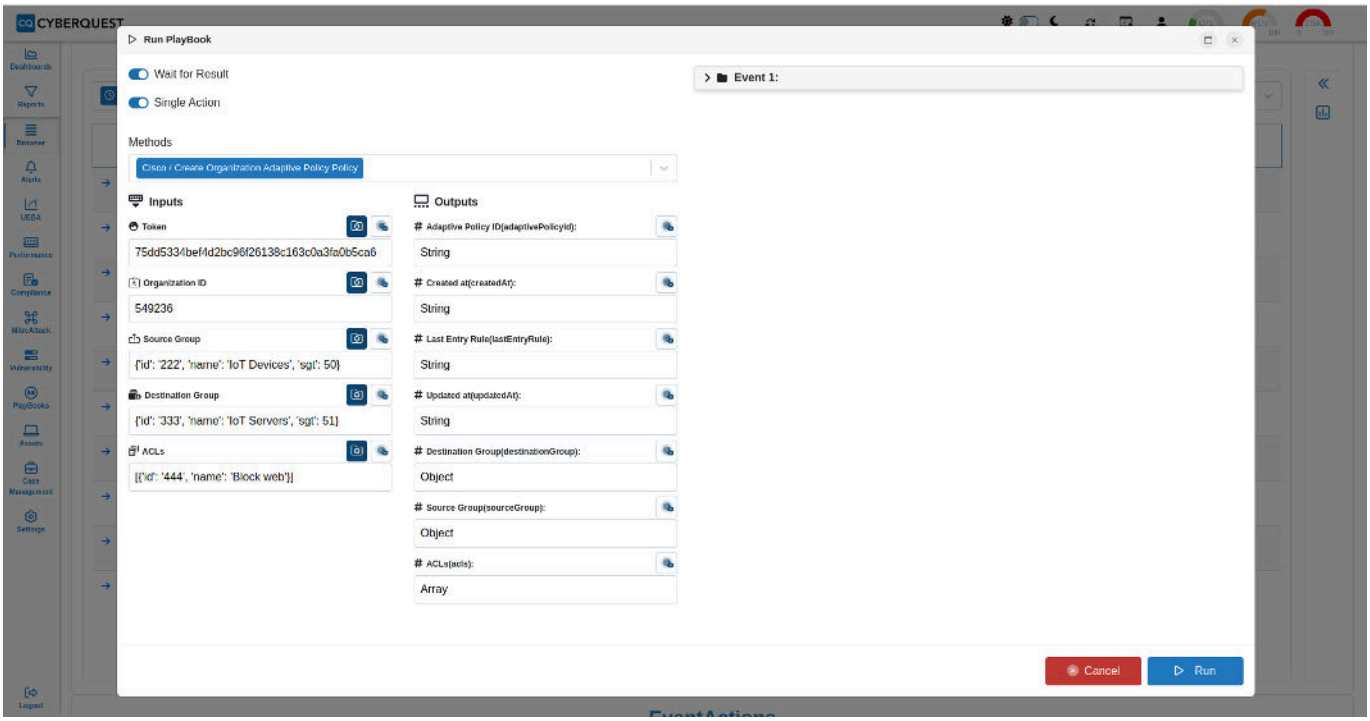


Inputs	Description
Token (is required)	To use the Cisco API, you must have an API key.
Organization ID (is required)	The ID of the Organization
Group ID (is required)	The ID of the adaptive policy group

Outputs	Description

Cisco/Create Organization Adaptive Policy Policy method

Add an Adaptive Policy.

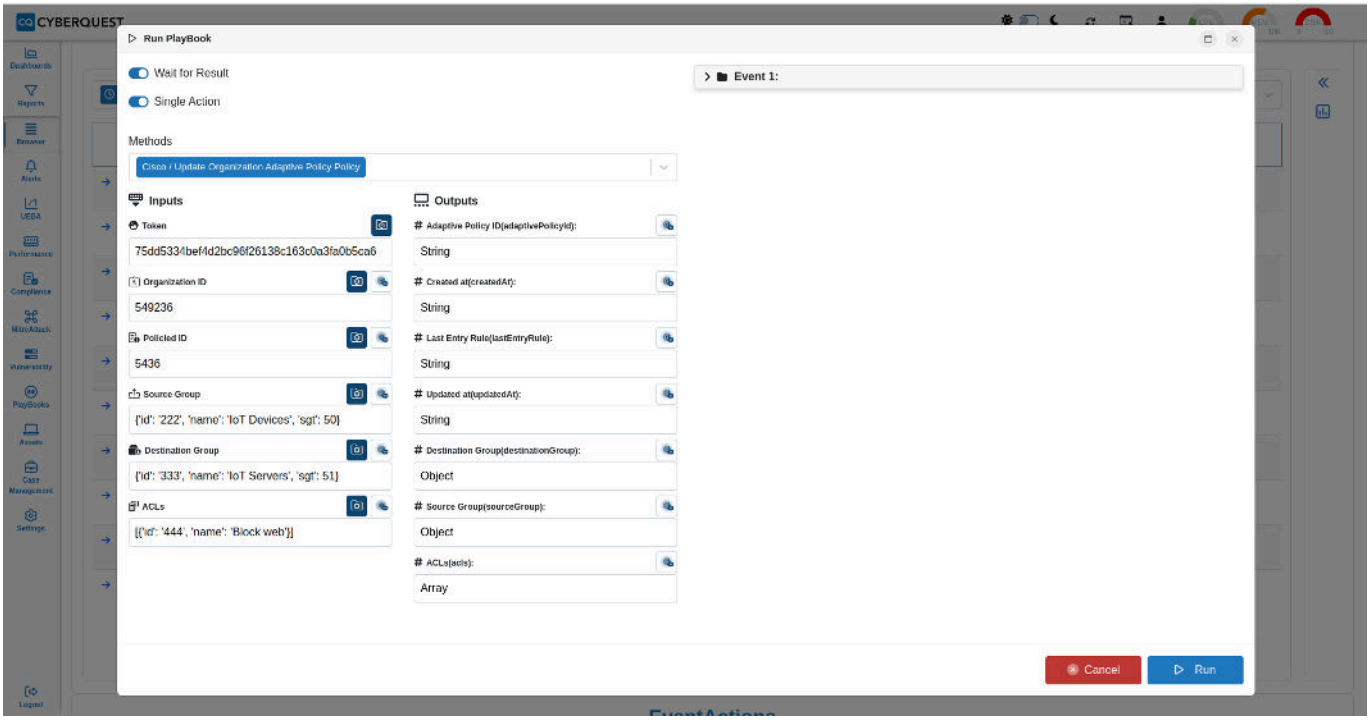


Inputs	Description
Token (is required)	To use the Cisco API, you must have an API key.
Organization ID (is required)	The ID of the Organization
Source Group (is required)	The source adaptive policy group (requires one unique attribute)
Destination Group (is required)	The destination adaptive policy group (requires one unique attribute)
ACLs (is required)	An ordered array of adaptive policy ACLs (each requires one unique attribute) that apply to this policy (default: [ ])

Outputs	Description
Adaptive Policy ID (adaptivePolicyId)	The ID for the adaptive policy
Created at (createdAt)	The created at timestamp for the adaptive policy
Last Entry Rule (lastEntryRule)	The rule to apply if there is no matching ACL
Updated at (updatedAt)	The updated at timestamp for the adaptive policy
Destination Group (destinationGroup)	The destination group for the given adaptive policy
Source Group (sourceGroup)	The source group for the given adaptive policy
ACLs (acls)	The access control lists for the adaptive policy

Cisco/Update Organization Adaptive Policy Policy method

Update an Adaptive Policy.

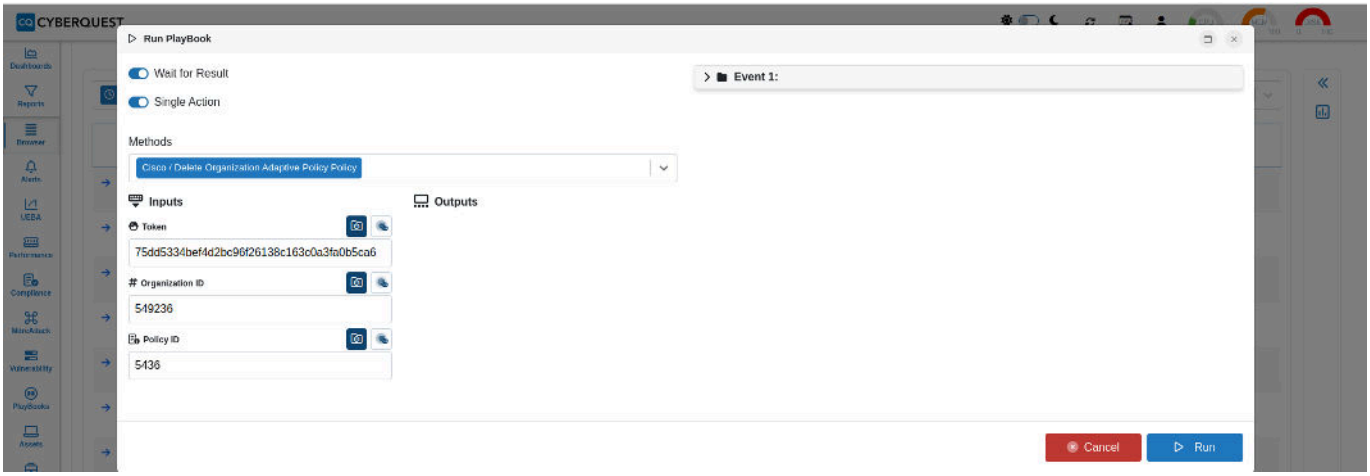


Inputs	Description
Token (is required)	
Organization ID (is required)	The ID of the Organization
Policied ID (is required)	The ID of the policy
Source Group (is required)	The source adaptive policy group (requires one unique attribute)
Destination Group (is required)	The destination adaptive policy group (requires one unique attribute)
ACLs (is required)	An ordered array of adaptive policy ACLs (each requires one unique attribute) that apply to this policy

Outputs	Description
Adaptive Policy ID (adaptivePolicyId)	The ID for the adaptive policy
Created at (createdAt)	The created at timestamp for the adaptive policy
Last Entry Rule (lastEntryRule)	The rule to apply if there is no matching ACL
Updated at (updatedAt)	The updated at timestamp for the adaptive policy
Destination Group (destinationGroup)	The destination group for the given adaptive policy
Source Group (sourceGroup)	The source group for the given adaptive policy
ACLs (acls)	The access control lists for the adaptive policy

Cisco/Delete Organization Adaptive Policy Policy method

Delete an Adaptive Policy.



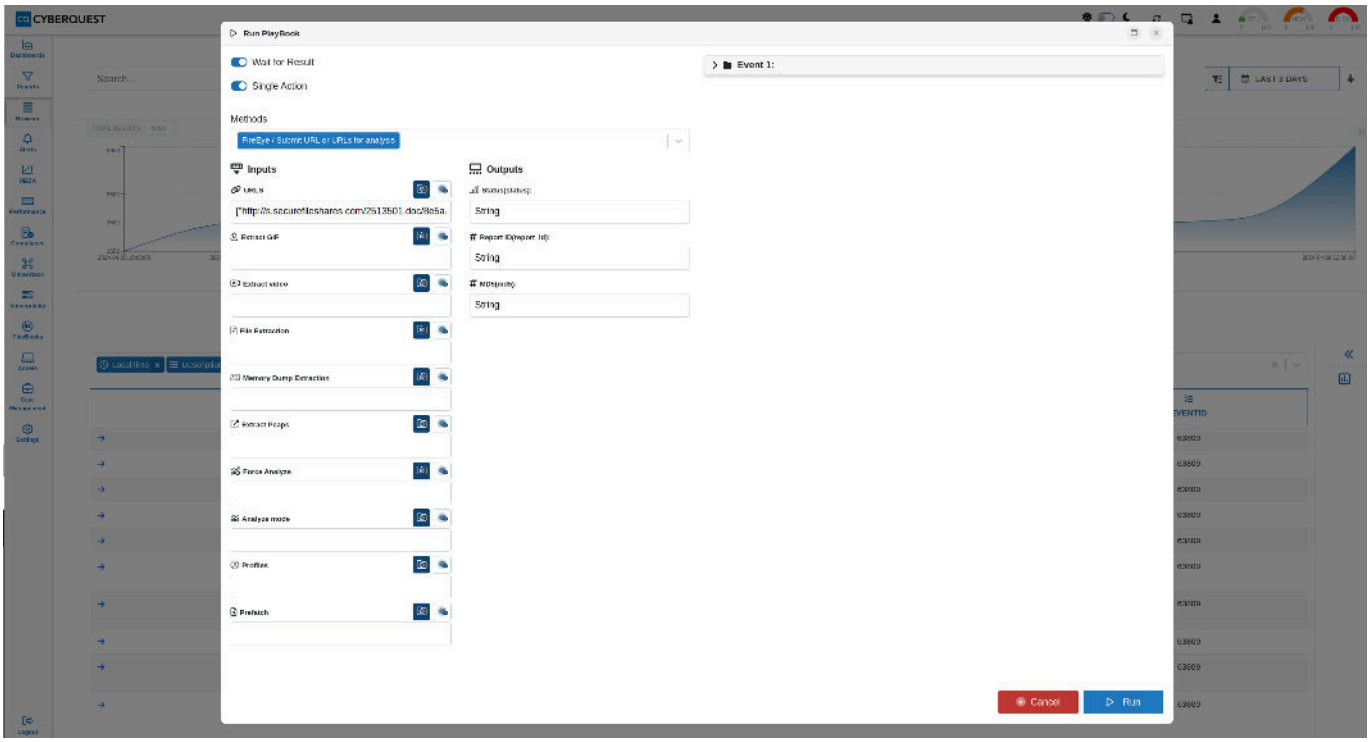
Inputs	Description
Token (is required)	To use the Cisco API, you must have an API key.
Organization ID (is required)	The ID of the Organization
Policy ID (is required)	The ID of the policy which will be deleted

Outputs	Description

FireEye

FireEye/Submit URL or URLs for analysis method

This endpoint submits a list of URLs for analysis. The limit is 5 URLs in a single call.

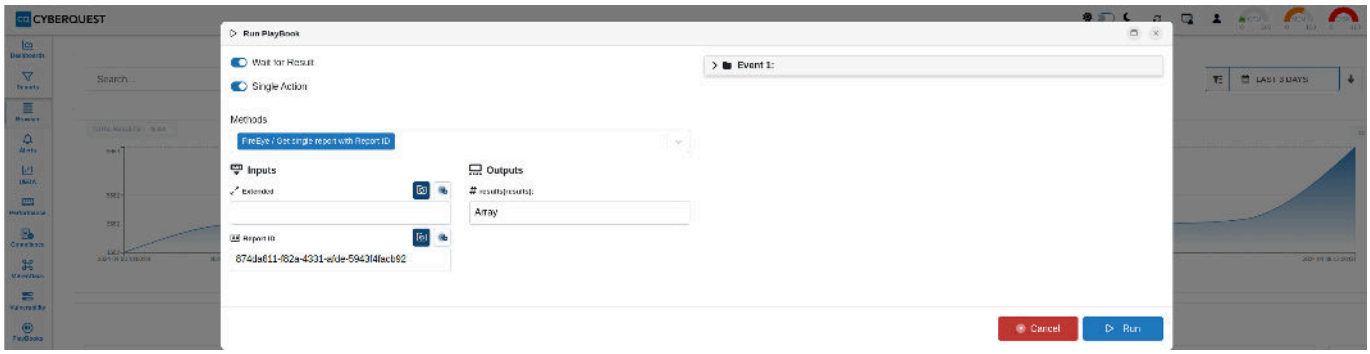


Inputs	Description
URLS (is required)	This is the list of URLs to submit for analysis in the form of ['url1','url2',...]. Maximum of 10 URLs allowed
Extract GIF	Extract screenshot of screen activity during dynamic analysis if true, which later can be downloaded with artifacts api
Extract video	Extract video activity during dynamic analysis if true, which later can be downloaded with artifacts api
File Extraction	Extract dropped files from vm during dynamic analysis if true, which later can be downloaded with artifacts api
Memory Dump Extraction	Extract video activity during dynamic analysis if true, which later can be downloaded with artifacts api
Extract Pcaps	Extract memory dump files from vm during dynamic analysis if true, which later can be downloaded with artifacts api
Force Analyze	Force submission for this url even if found as duplicate
Analyze mode	Analysis mode for submission(live). If analysis mode is set to live then profiles have to be provided
Profiles	Profiles to be used if analysis_mode is set to live
Prefatch	Download and analyze any file that the url points to

Outputs	Description
Status (status)	This means that your file has been received and stored successfully. This does not mean your analysis has started or was completed–you will need to check the report for this report ID to see the analysis status
Report ID (report_id)	This is the analysis job ID of your file submission. Use this value as the report_id parameter in GET /reports/{report_id}. You will need to keep your own database of your report IDs to view your reports and their status as the report IDs cannot be retrieved at a later time
MD5 (md5)	Returned NA in case of urls

FireEye/Get single report with Report ID method

This endpoint fetches the results of a single file submission, known as a report.

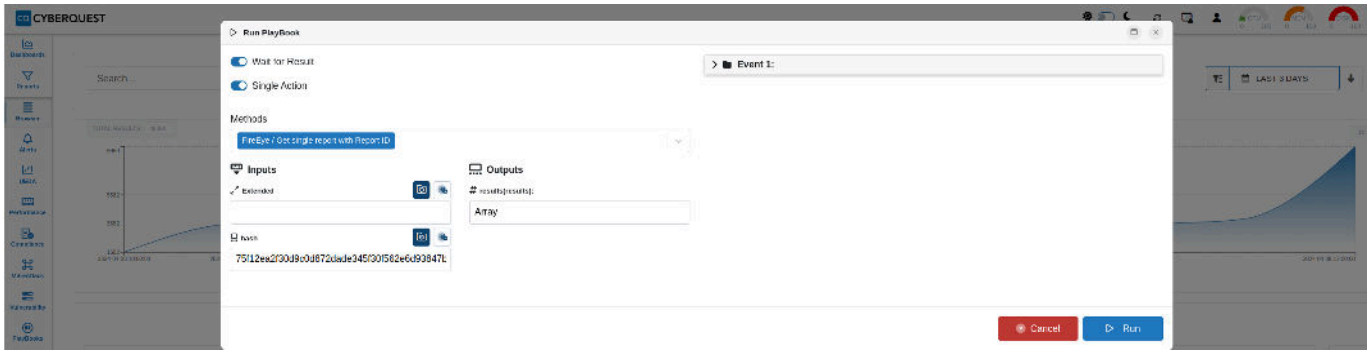


Inputs	Description
Extended	Setting extended to true will allow you to see all malware engine reports.
Report ID (is required)	The report ID returned after successfully submitting a file.

Outputs	Description
results (results)	The results of the API call

FireEye/Get single report with Hash method

This endpoint fetches the latest results for file submission with the provided md5 or sha256 hash.

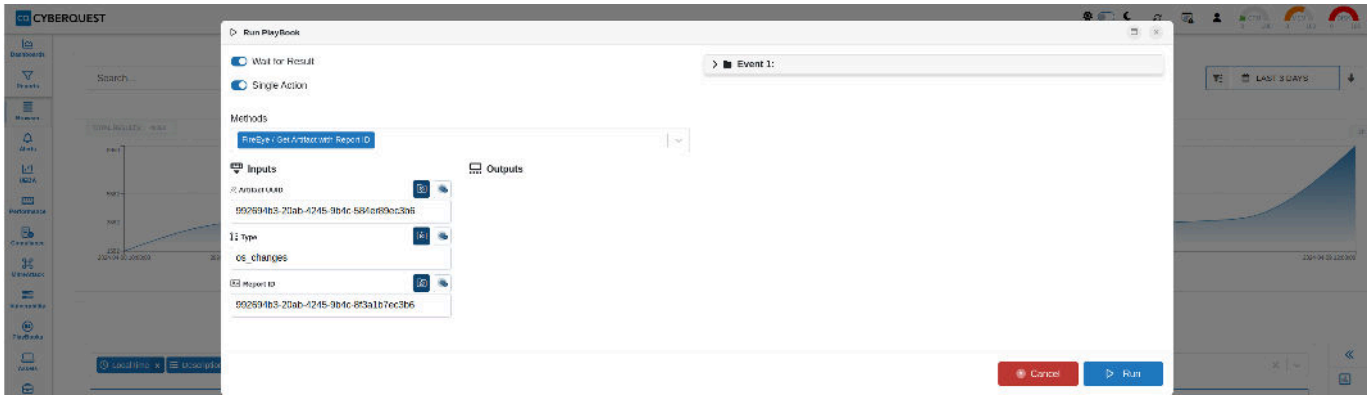


Inputs	Description
Extended	Setting extended to true will allow you to see all malware engine reports.
hash (is required)	MD5 or SHA256 hash of a submitted file

Outputs	Description
results (results)	The results of the API call

FireEye/Get Artifact with Report ID method

This endpoint fetches artifacts, like a screenshot gif file, for the given report_id.

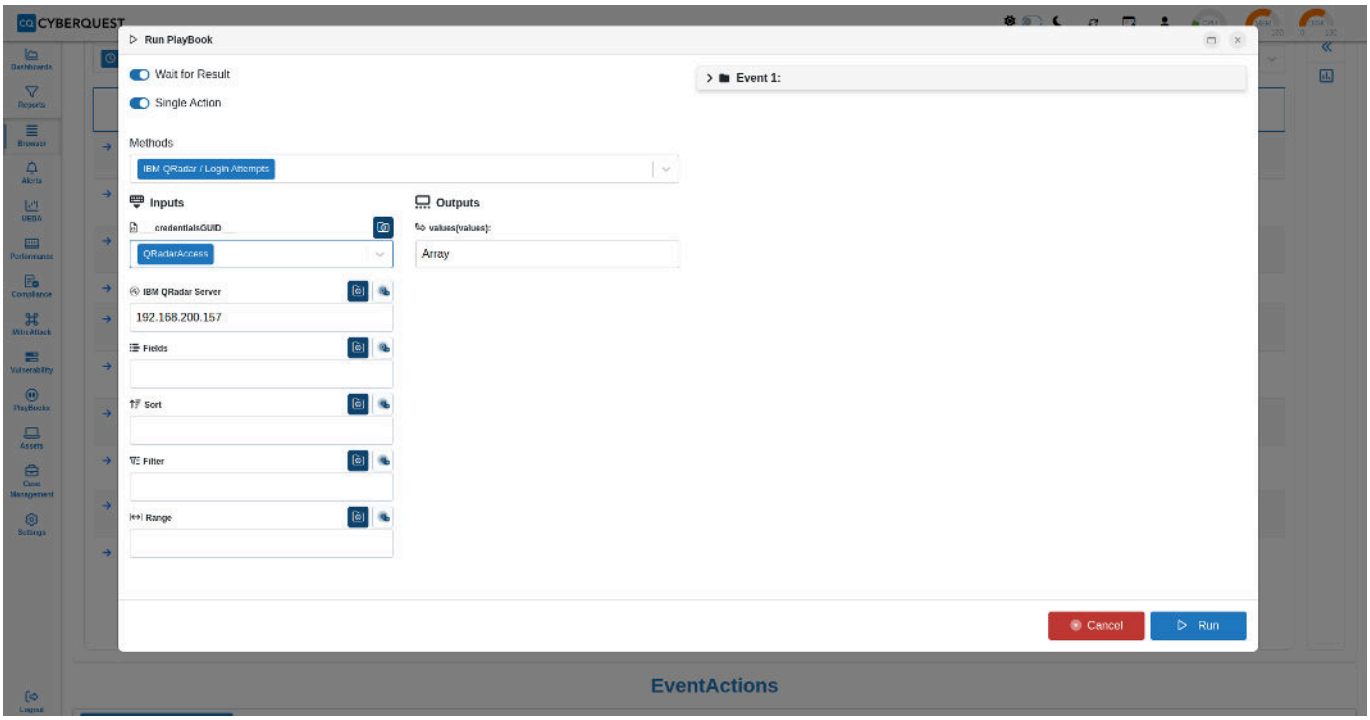


Inputs	Description
Artifact UUID	Submitted sample can have more that one artifacts each artifact will have its on artifact uuid which is reported as part of reports api. User need to grab artifacts uuid from reports endpoint.
Type (is required)	Type of artifact to download.
Report ID (is required)	The report ID returned after successfully submitting a file.

IBM QRadar

IBM QRadar/Login Attempts method

Gets the list of login attempts. For SAAS and single signon authentication modules, failed login attempts will not be tracked. The successful login attempts will be created when the QRadar session is created, not necessarily when the user entered their credentials on the single sign on login page. Any users or authorized service can call this endpoint. If the caller has the ADMIN capability, login attempts for all users will be returned. For all other callers, only login attempts for the current caller will be returned.

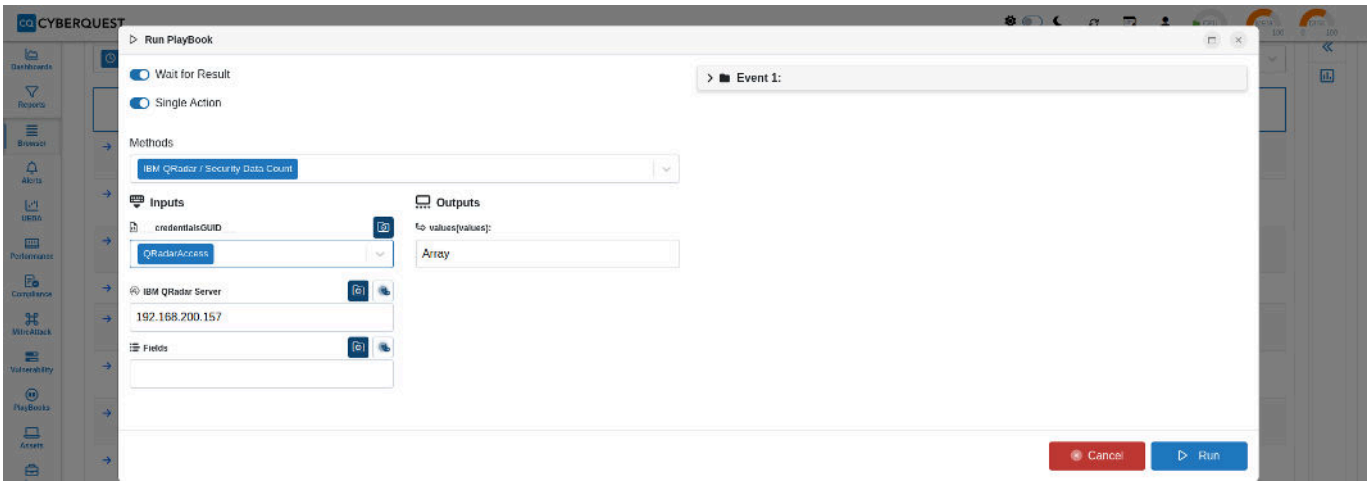


Inputs	Description
credentialsGUID (is required)	
IBM QRadar Server (is required)	The server where the IBM QRadar is installed
Fields	Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Sort	This parameter is used to sort the elements in a list.
Filter	This parameter is used to restrict the elements in a list base on the contents of various fields.
Range	Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.

Outputs	Description
values (values)	The results of the API call

IBM QRadar/Security Data Count method

Retrieves count of security artifacts in QRadar.

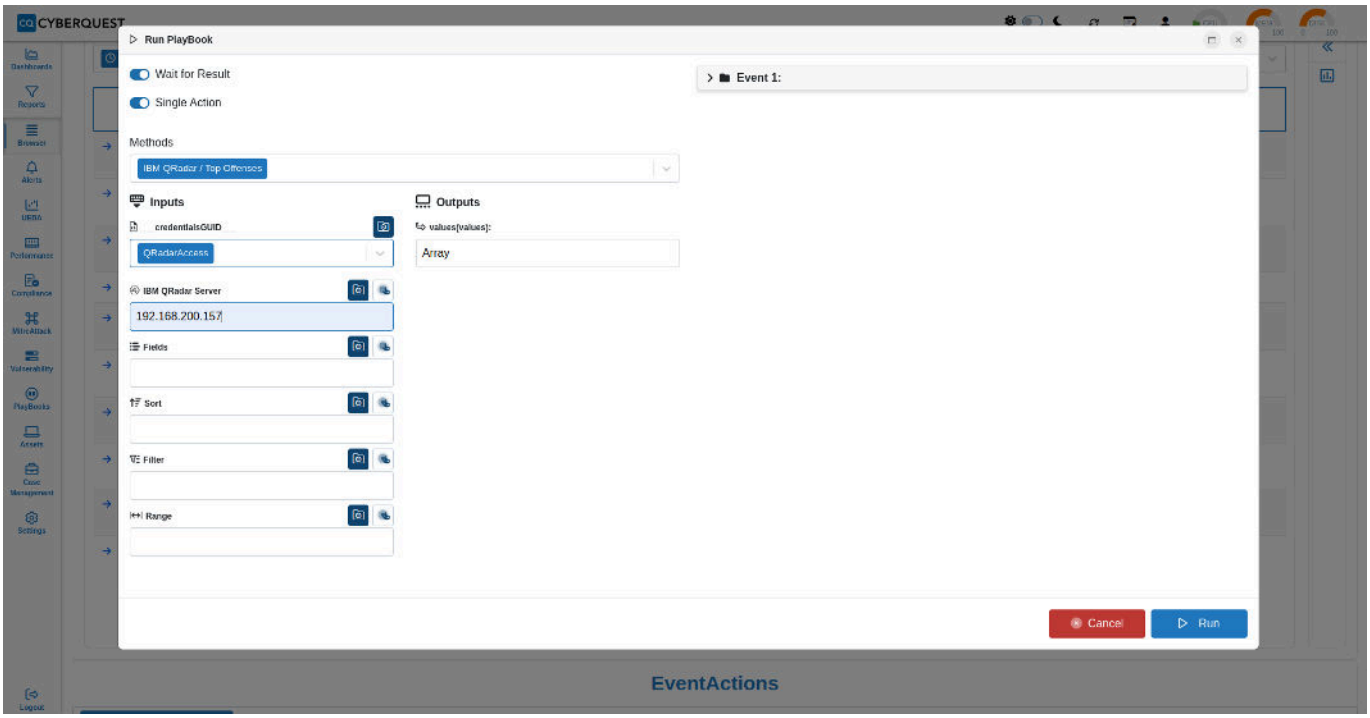


Inputs	Description
credentialsGUID (is required)	
IBM QRadar Server (is required)	The server where the IBM QRadar is installed
Fields	Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Outputs	Description
values (values)	The results of the API call

IBM QRadar/Top Offenses method

Retrieves Top Offenses in the system sorted by update count.

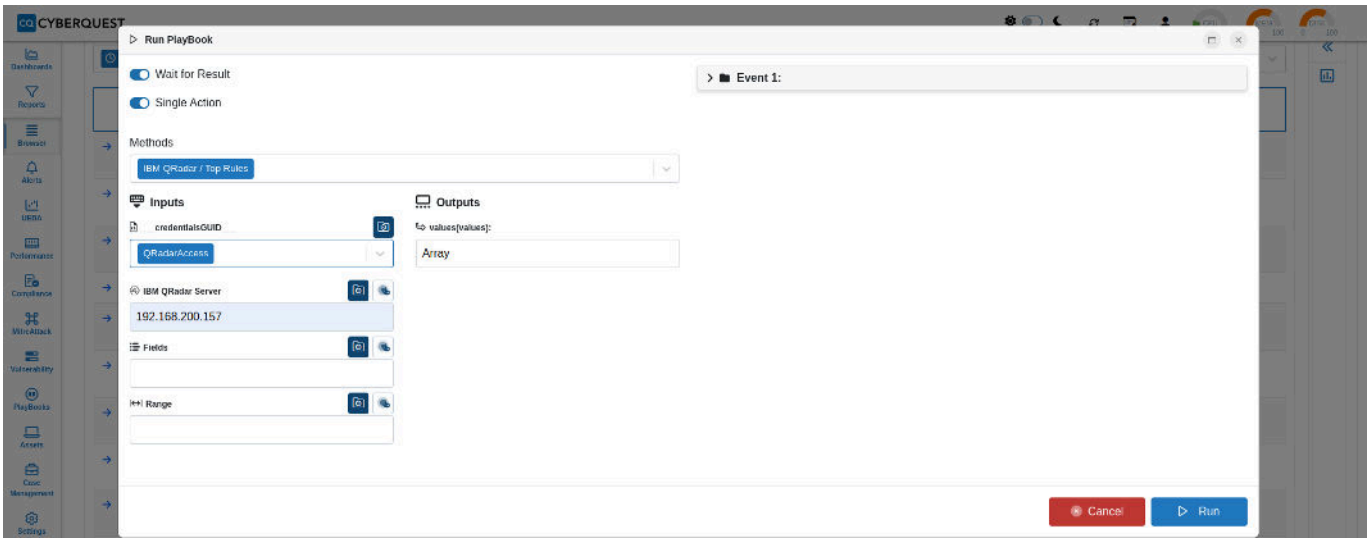


Inputs	Description
credentialsGUID (is required)	
IBM QRadar Server (is required)	The server where the IBM QRadar is installed
Fields	Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Sort	This parameter is used to sort the elements in a list.
Filter	This parameter is used to restrict the elements in a list base on the contents of various fields.
Range	Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.

Outputs	Description
values (values)	The results of the API call

IBM QRadar/Top Rules method

Retrieves Top Rules in the system sorted by response count.

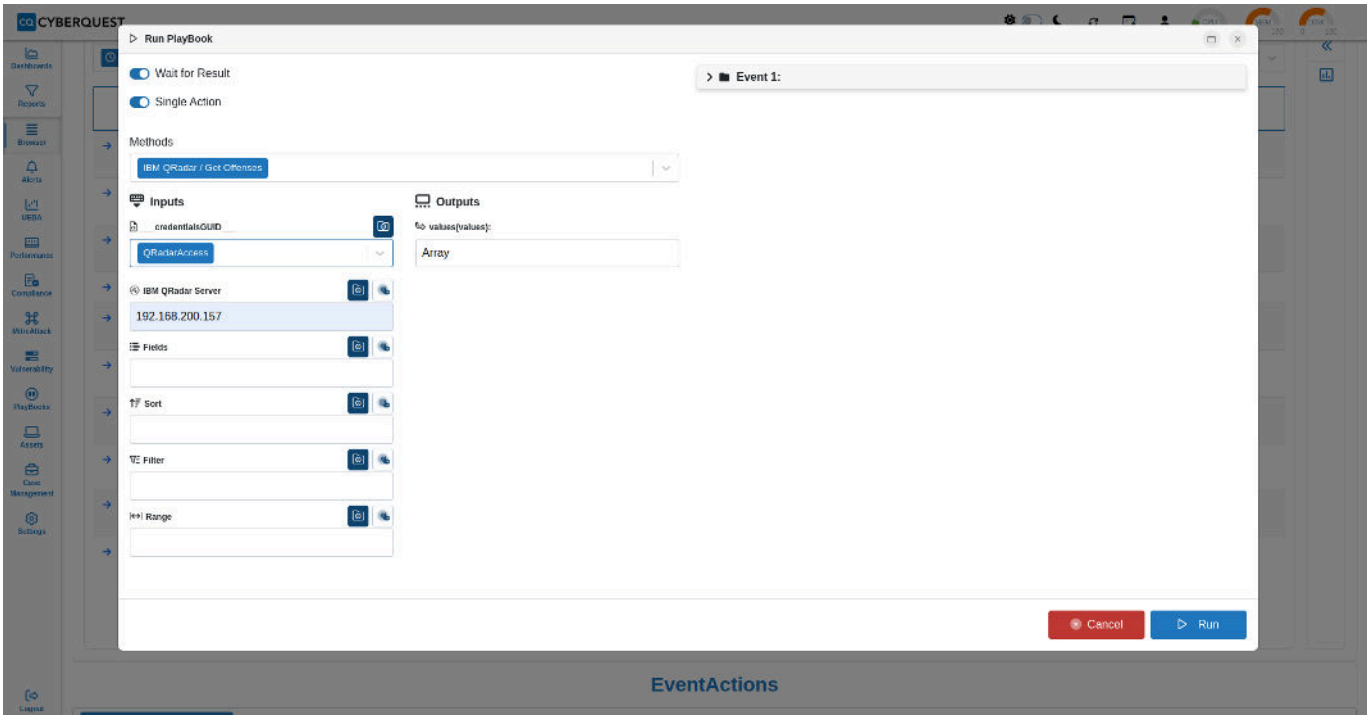


Inputs	Description
credentialsGUID (is required)	
IBM QRadar Server (is required)	The server where the IBM QRadar is installed
Fields	Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Range	Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.

Outputs	Description
values (values)	The results of the API call

IBM QRadar/Get Offenses method

Retrieve a list of offenses currently in the system.

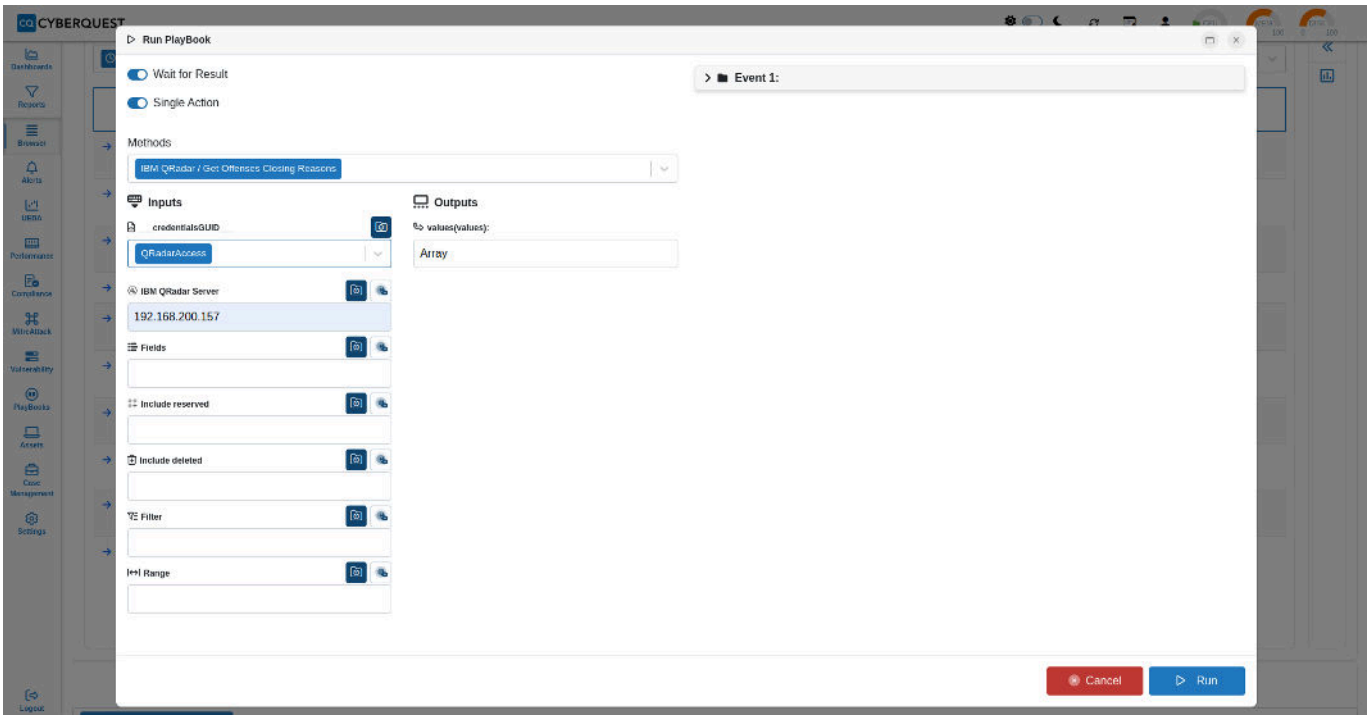


Inputs	Description
credentialsGUID (is required)	
IBM QRadar Server (is required)	The server where the IBM QRadar is installed
Fields	Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Sort	This parameter is used to sort the elements in a list.
Filter	This parameter is used to restrict the elements in a list base on the contents of various fields.
Range	Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.

Outputs	Description
values (values)	The results of the API call

IBM QRadar/Get Offenses Closing Reasons method

Retrieve a list of all offense closing reasons.

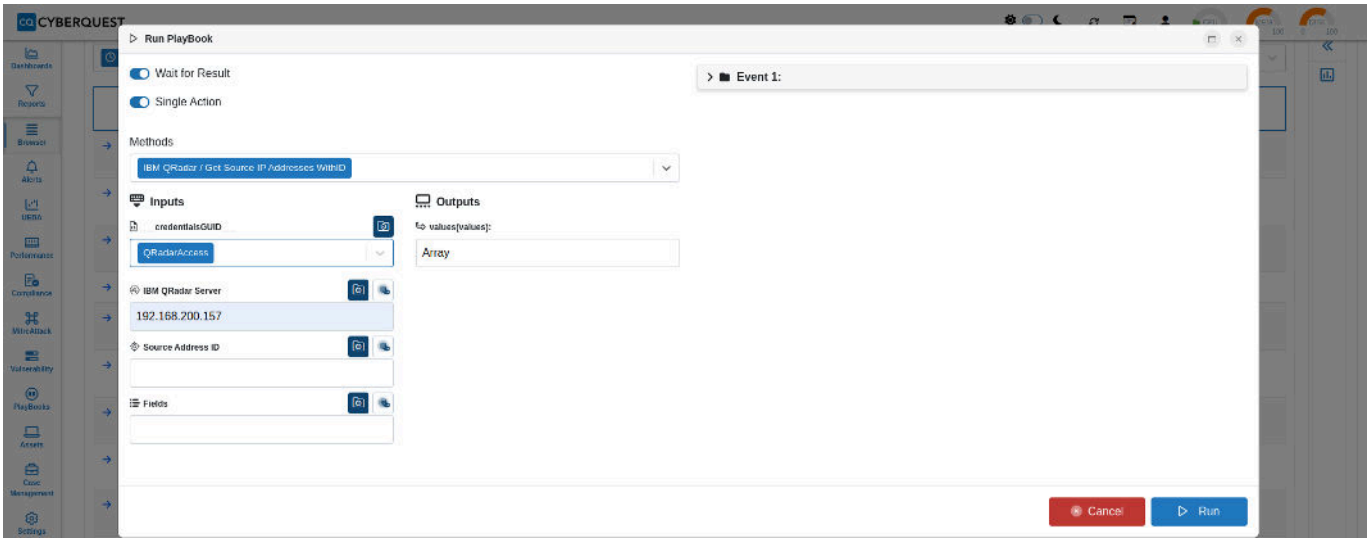


Inputs	Description
credentialsGUID (is required)	
IBM QRadar Server (is required)	The server where the IBM QRadar is installed
Fields	Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Include reserved	f true, reserved closing reasons are included in the response. Defaults to false. Reserved closing reasons cannot be used to close an offense.
Include deleted	If true, deleted closing reasons are included in the response. Defaults to false. Deleted closing reasons cannot be used to close an offense.
Filter	This parameter is used to restrict the elements in a list base on the contents of various fields.
Range	Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.

Outputs	Description
values (values)	The results of the API call

IBM QRadar/Get Source IP Addresses WithID method

Retrieve an offense source address.

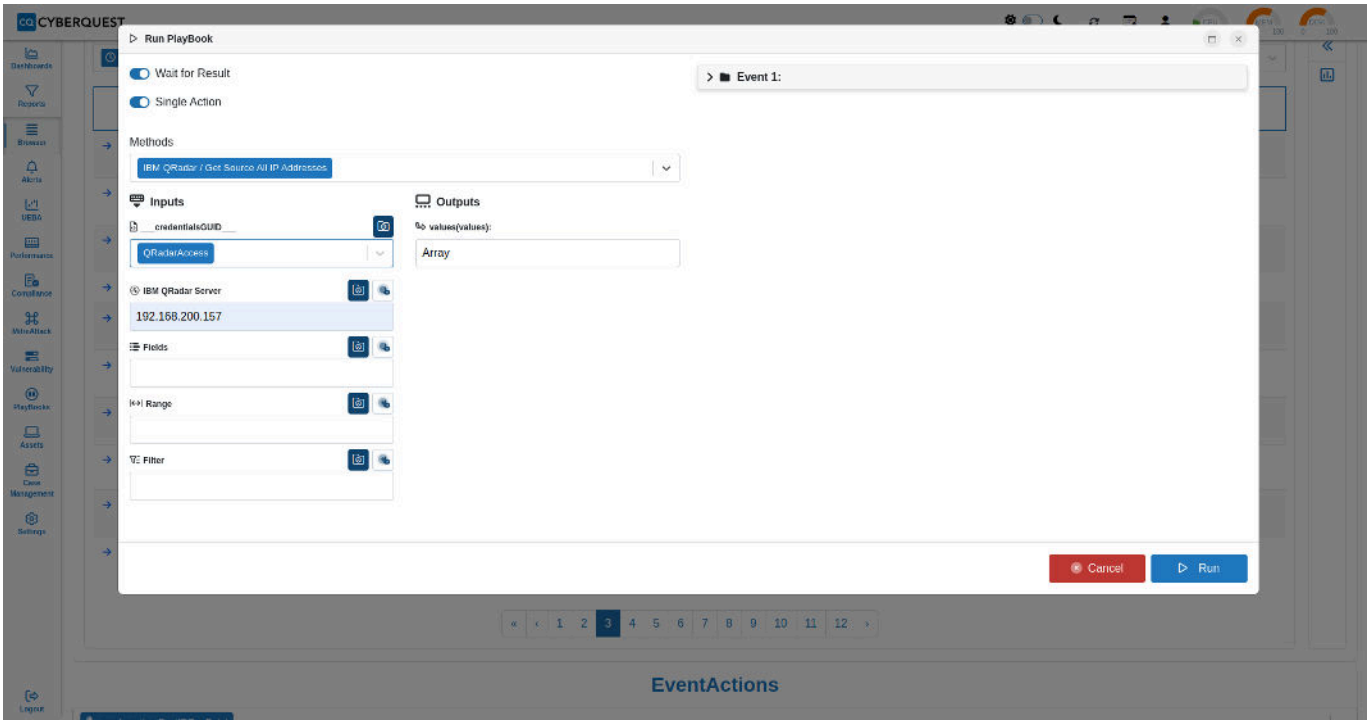


Inputs	Description
credentialsGUID (is required)	
IBM QRadar Server (is required)	The server where the IBM QRadar is installed
Source Address ID (is required)	The ID of the source address to retrieve.
Fields	Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Outputs	Description
values (values)	The results of the API call

IBM QRadar/Get Source All IP Addresses method

Retrieve a list offense source addresses currently in the system.

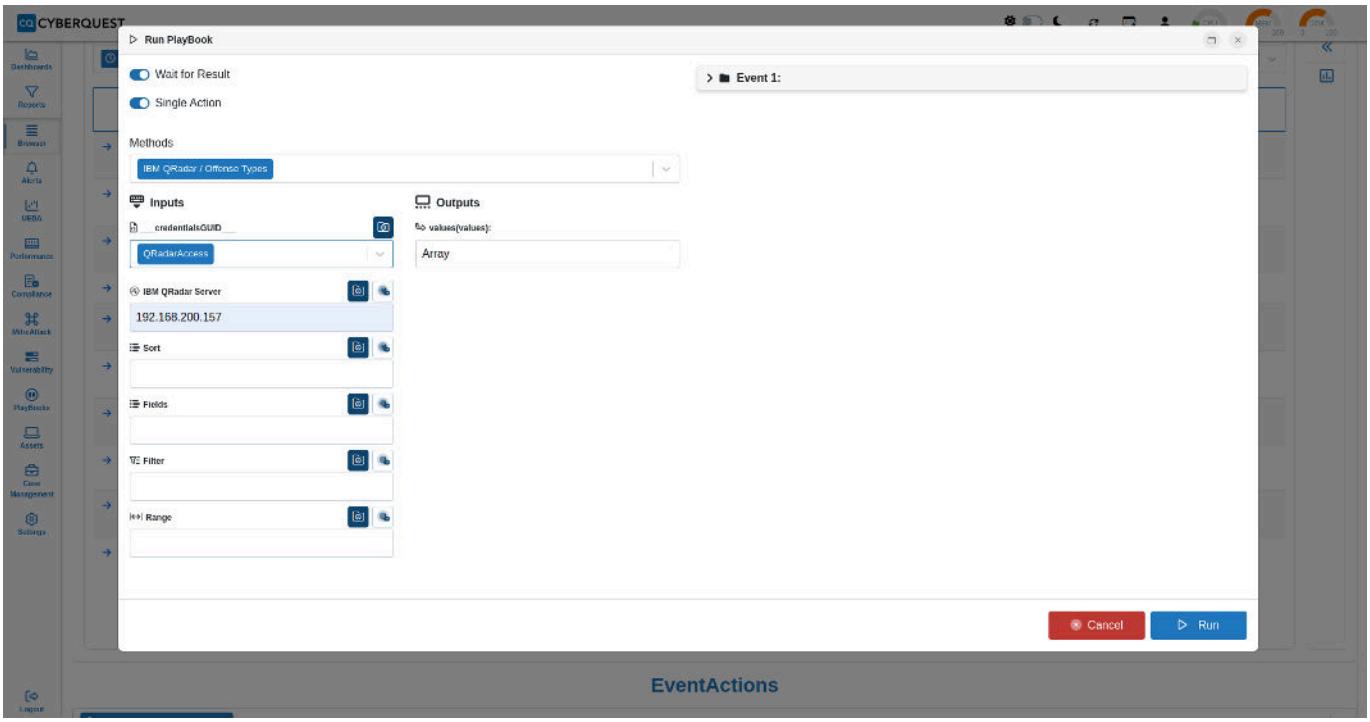


Inputs	Description
credentialsGUID (is required)	
IBM QRadar Server (is required)	The server where the IBM QRadar is installed
Fields	Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Range	Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
Filter	This parameter is used to restrict the elements in a list base on the contents of various fields.

Outputs	Description
values (values)	The results of the API call

IBM QRadar/Offense Types method

Retrieve all the Offense Types.

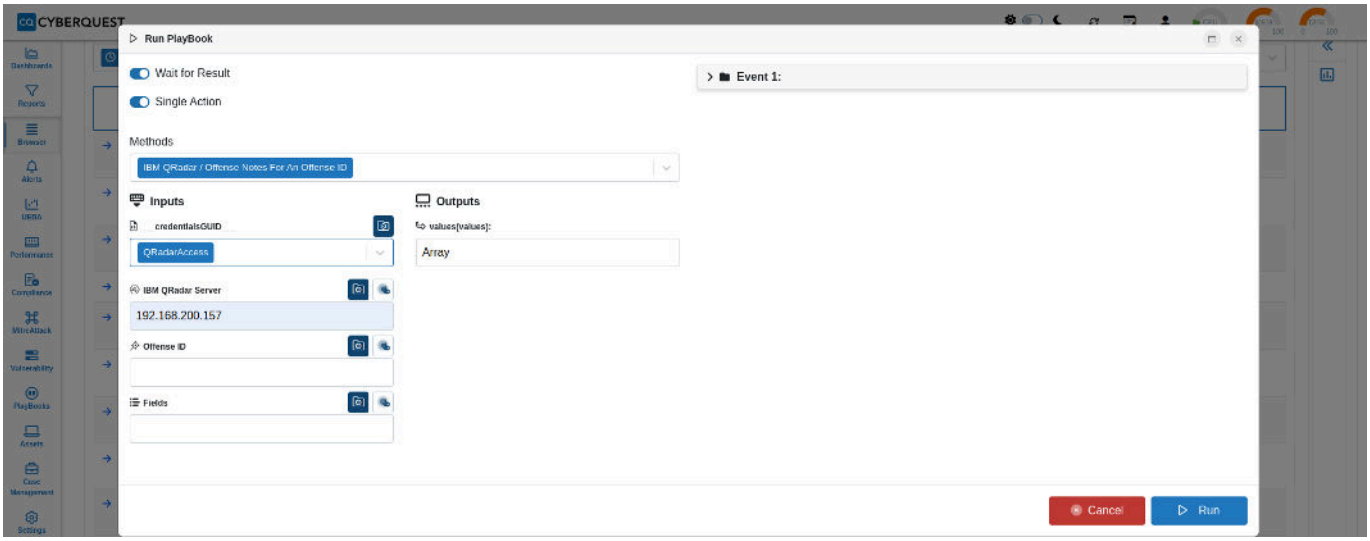


Inputs	Description
credentialsGUID (is required)	
IBM QRadar Server (is required)	The server where the IBM QRadar is installed
Sort	This parameter is used to sort the elements in a list.
Fields	Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Filter	This parameter is used to restrict the elements in a list base on the contents of various fields.
Range	Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.

Outputs	Description
values (values)	The results of the API call

IBM QRadar/Offense Notes For An Offense ID method

Retrieve a list of notes for an offense.

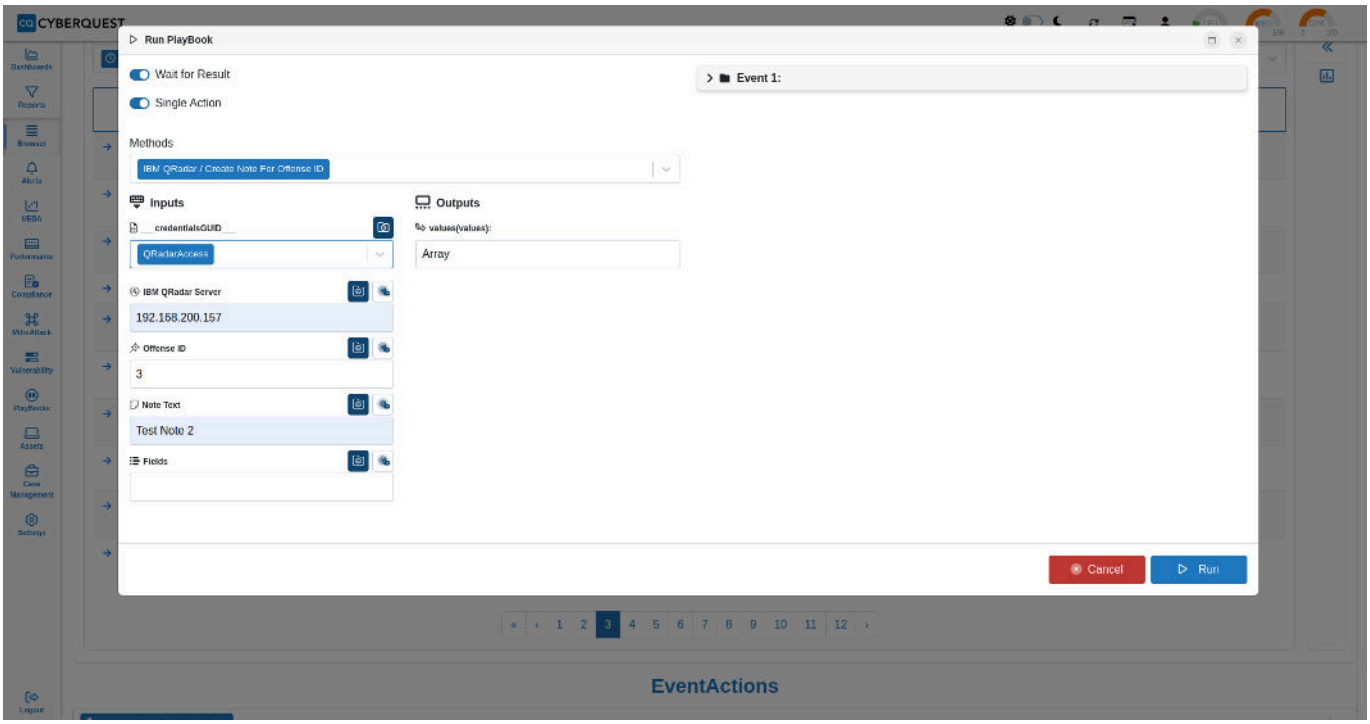


Inputs	Description
credentialsGUID (is required)	
IBM QRadar Server (is required)	The server where the IBM QRadar is installed
Offense ID (is required)	The offense ID to retrieve the notes for.
Fields	Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Outputs	Description
values (values)	The results of the API call

IBM QRadar/Create Note For Offense ID method

Create a note on an offense.

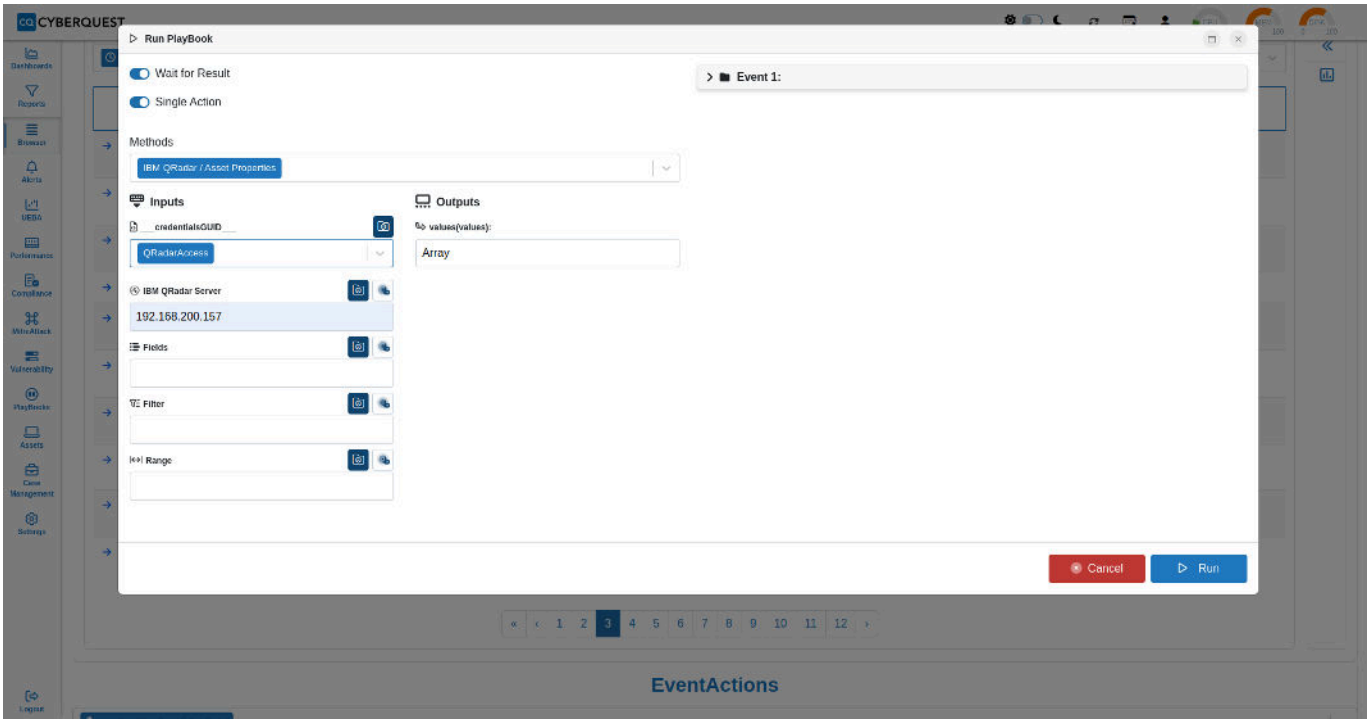


Inputs	Description
credentialsGUID (is required)	
IBM QRadar Server (is required)	The server where the IBM QRadar is installed
Offense ID (is required)	The offense ID to retrieve the notes for.
Note Text (is required)	The note text.
Fields	Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Outputs	Description
values (values)	The results of the API call

IBM QRadar/Asset Properties method

Get a list of available asset property types that can be used.

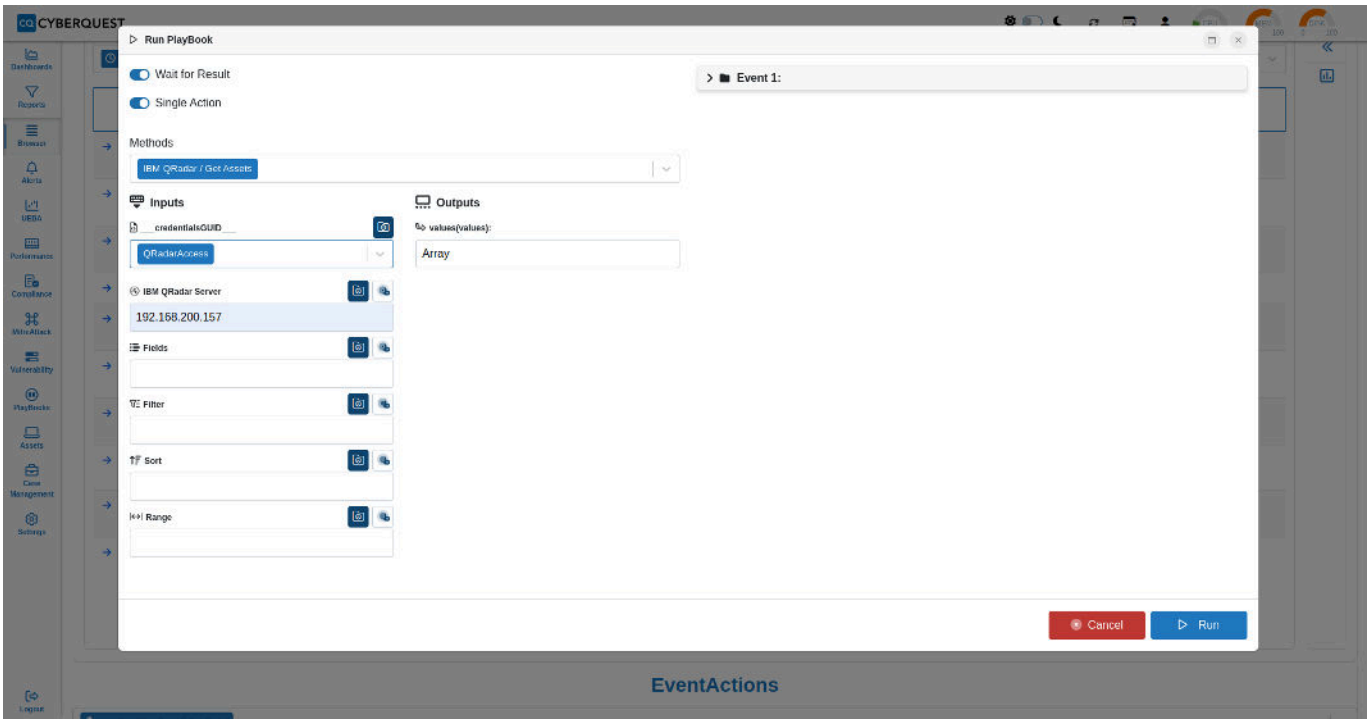


Inputs	Description
credentialsGUID (is required)	
IBM QRadar Server (is required)	The server where the IBM QRadar is installed
Fields	Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Filter	This parameter is used to restrict the elements in a list base on the contents of various fields
Range	Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.

Outputs	Description
values (values)	The results of the API call

IBM QRadar/Get Assets method

List all assets found in the model. This endpoint supports sorting on id, domain_id, vulnerability_count and risk_score_sum, and filtering on all fields. EXCEPTION: LIKE, ILIKE, and BETWEEN do not work on the interfaces(ip_addresses(value)) field. It is possible to use the inequality operators to work around this in most cases. Use of the fields header to request only the necessary fields will improve API performance.

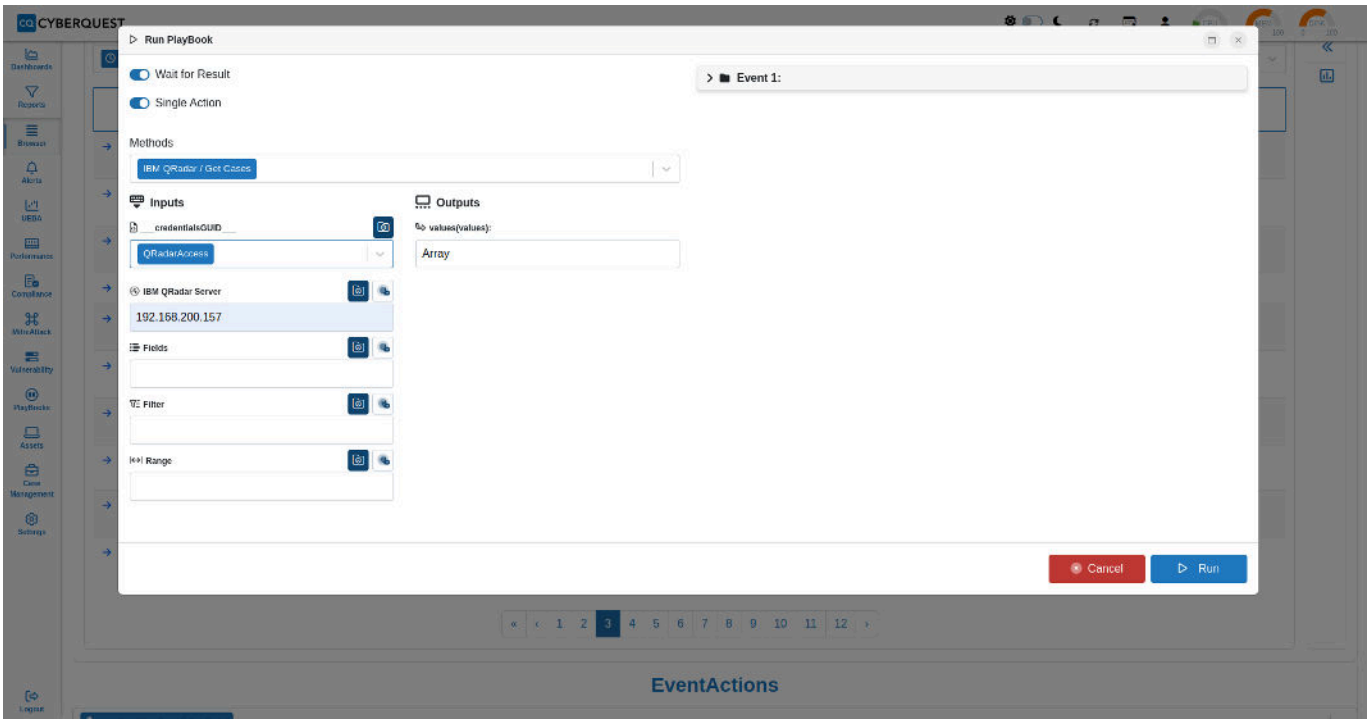


Inputs	Description
credentialsGUID (is required)	
IBM QRadar Server (is required)	The server where the IBM QRadar is installed
Fields	Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Filter	This parameter is used to restrict the elements in a list base on the contents of various fields
Sort	This parameter is used to sort the elements in a list.
Range	Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.

Outputs	Description
values (values)	The results of the API call

IBM QRadar/Get Cases method

Retrieves a list of cases.

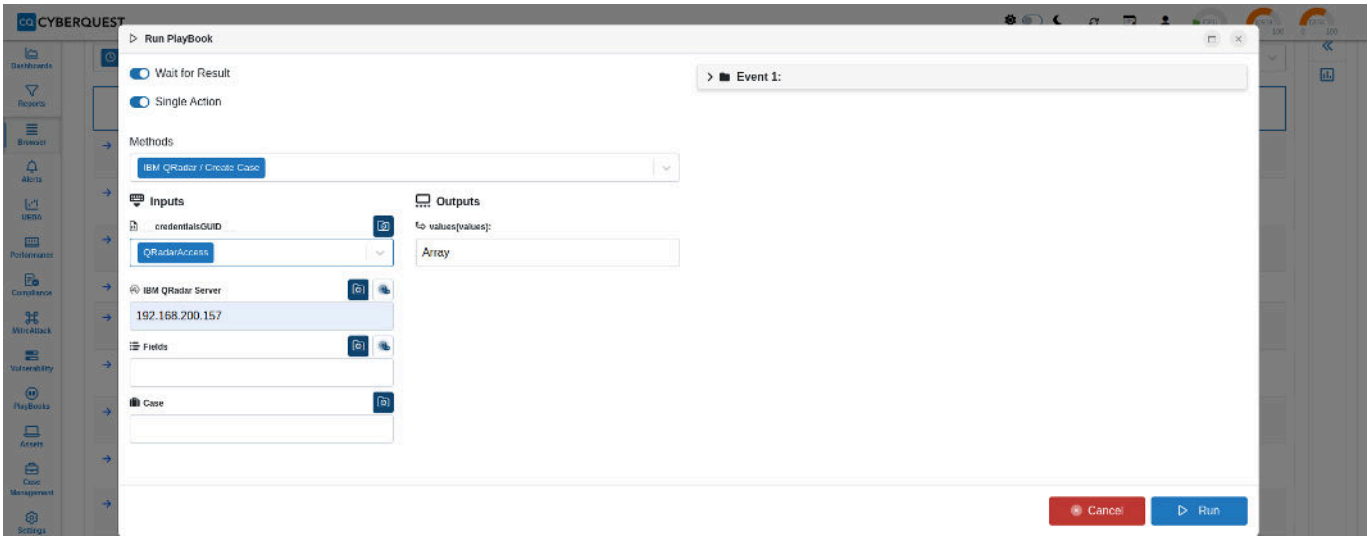


Inputs	Description
credentialsGUID (is required)	
IBM QRadar Server (is required)	The server where the IBM QRadar is installed
Fields	Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Filter	This parameter is used to restrict the elements in a list base on the contents of various fields
Range	Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.

Outputs	Description
values (values)	The results of the API call

IBM QRadar/Create Case method

Creates a new case.

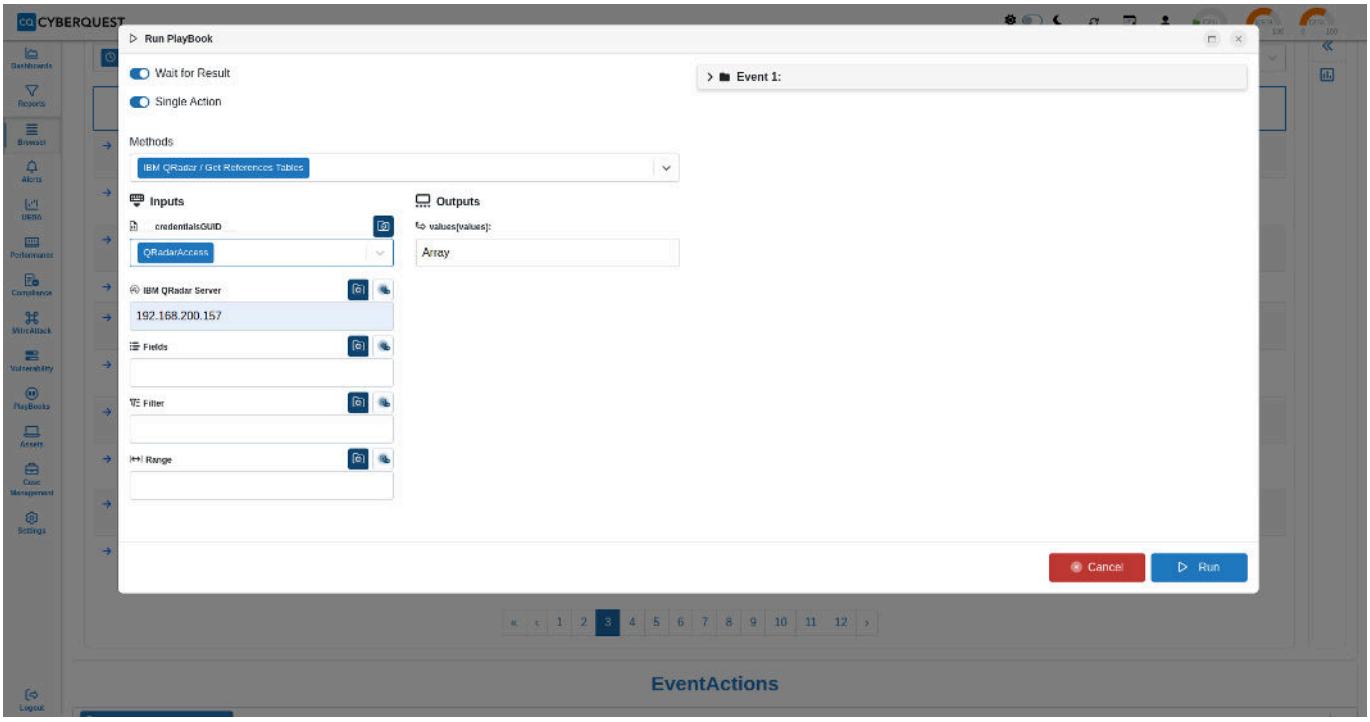


Inputs	Description
credentialsGUID (is required)	
IBM QRadar Server (is required)	The server where the IBM QRadar is installed
Fields	Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Case	

Outputs	Description
values (values)	The results of the API call

IBM QRadar/Get References Tables method

Retrieve a list of all reference tables.

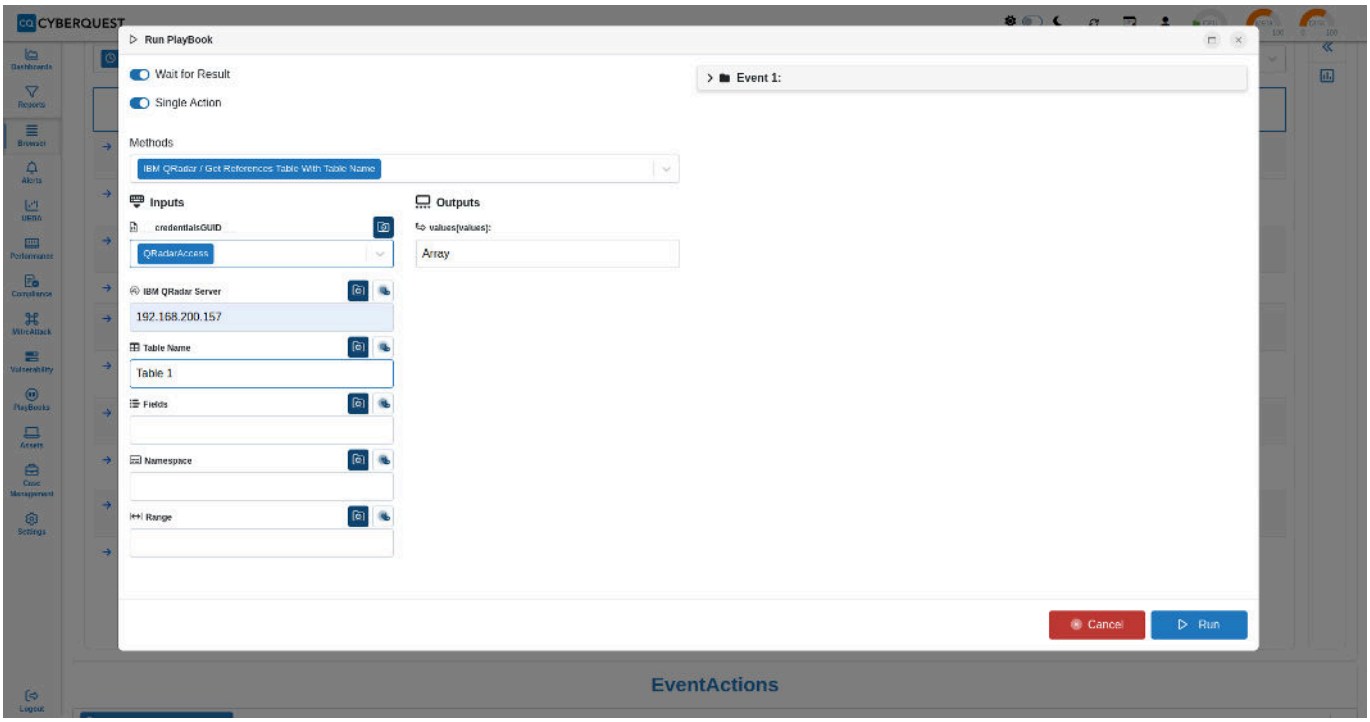


Inputs	Description
credentialsGUID (is required)	
IBM QRadar Server (is required)	The server where the IBM QRadar is installed
Fields	Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Filter	This parameter is used to restrict the elements in a list base on the contents of various fields
Range	Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.

Outputs	Description
values (values)	The results of the API call

IBM QRadar/Get References Table With Table Name method

Return the reference table identified by name.

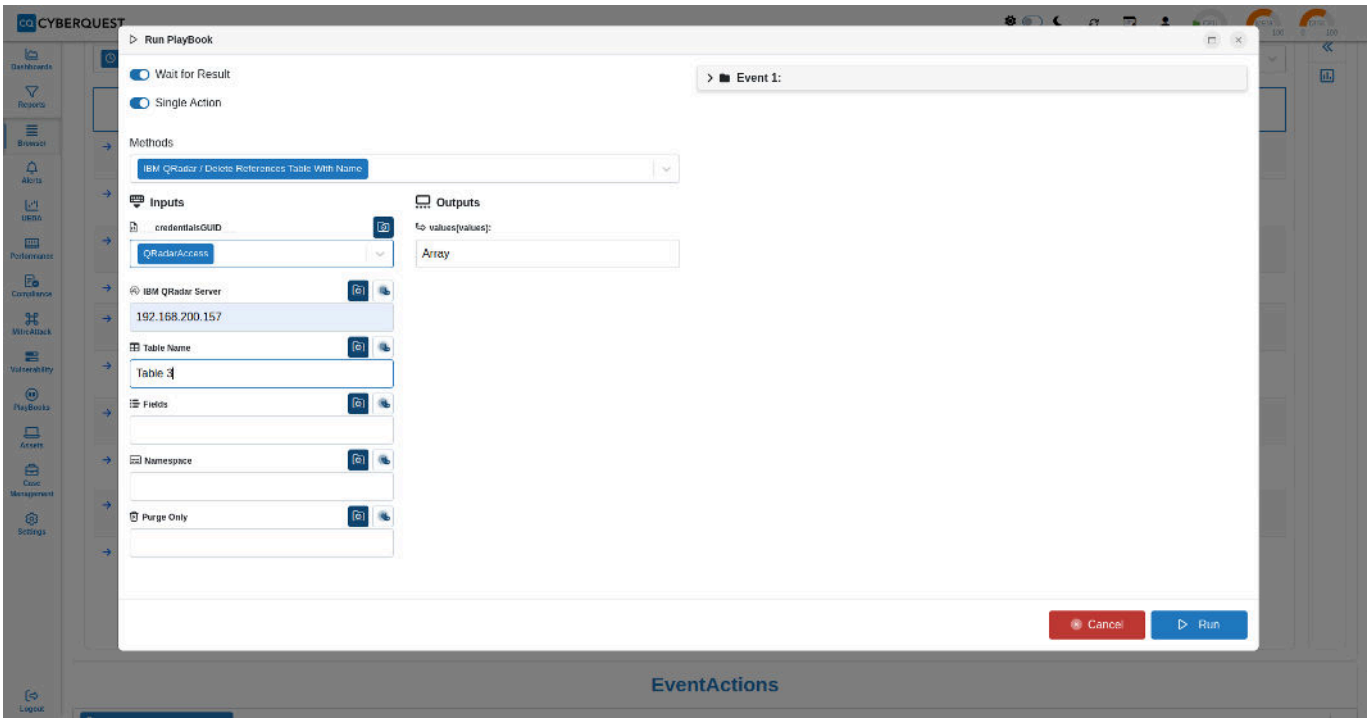


Inputs	Description
credentialsGUID (is required)	
IBM QRadar Server (is required)	The server where the IBM QRadar is installed
Table Name (is required)	Table identified by name.
Fields	Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Namespace	Either SHARED or TENANT, default is SHARED.
Range	Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.

Outputs	Description
values (values)	The results of the API call

IBM QRadar/Delete References Table With Name method

Remove a reference table or purge its contents.

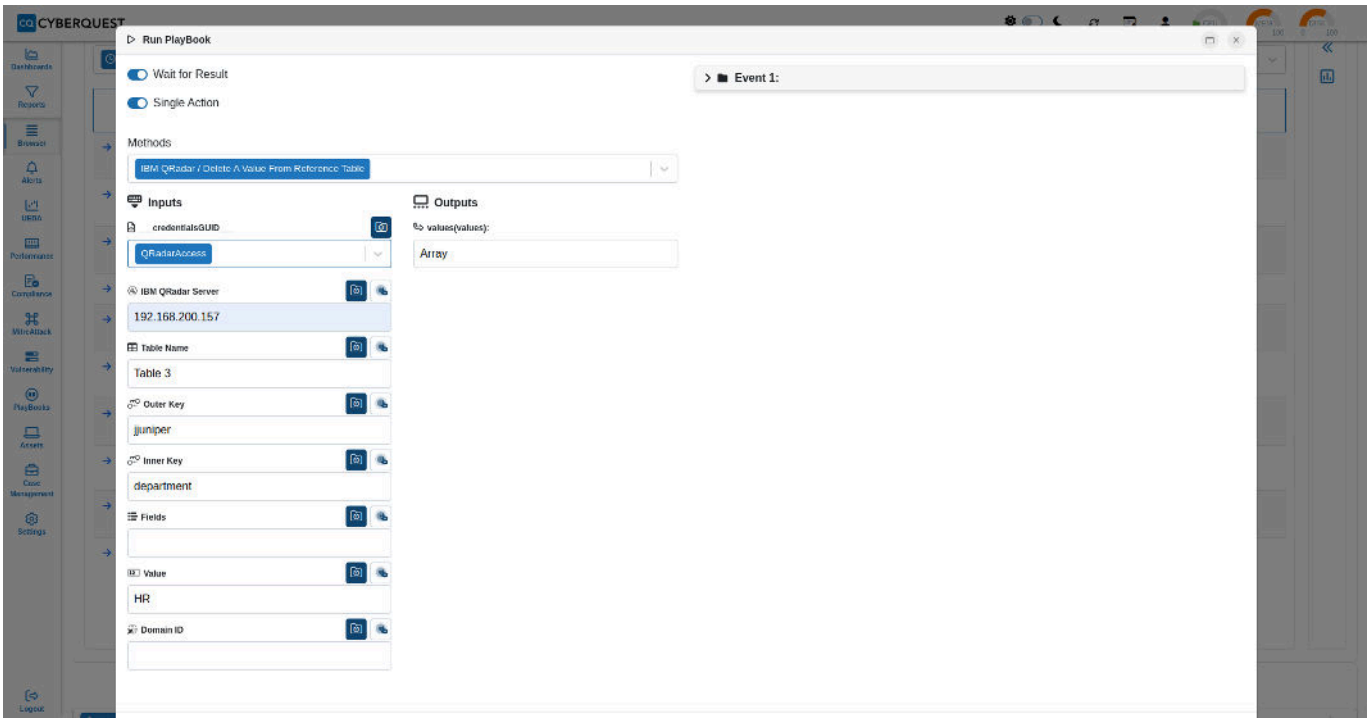


Inputs	Description
credentialsGUID (is required)	
IBM QRadar Server (is required)	The server where the IBM QRadar is installed
Table Name (is required)	Table identified by name.
Fields	Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Namespace	Either SHARED or TENANT, default is SHARED.
Purge Only	The allowed values are false or true. The default value is false. This indicates if the reference table should have its contents purged (true), keeping the reference table structure. If the value is false, or not specified the reference table is removed completely.

Outputs	Description
values (values)	The results of the API call

IBM QRadar/Delete A Value From Reference Table method

Remove a value from a reference table.

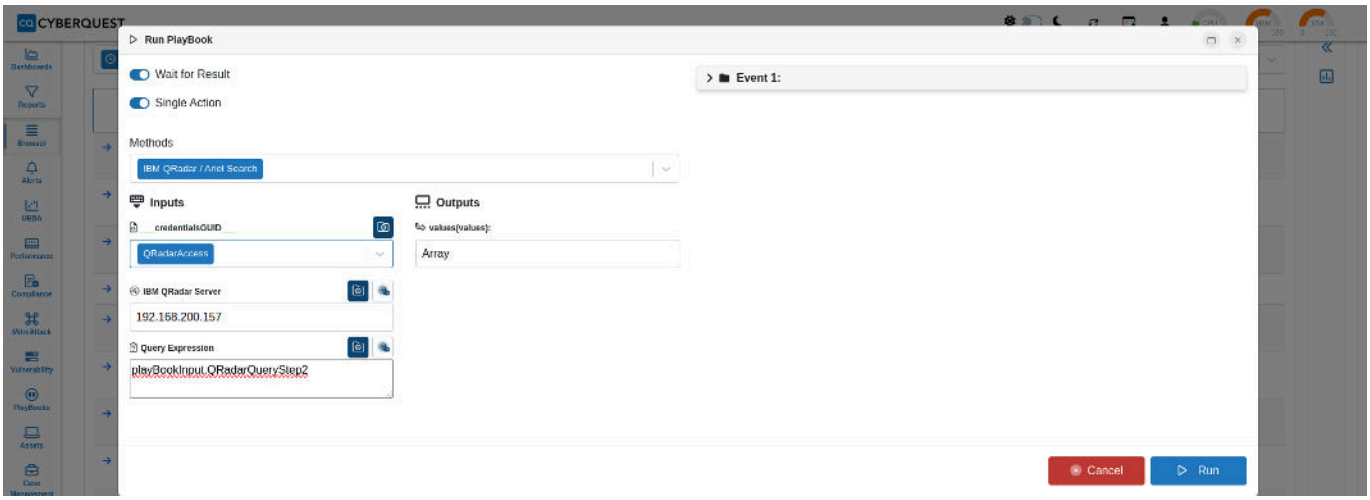


Inputs	Description
credentialsGUID (is required)	
IBM QRadar Server (is required)	The server where the IBM QRadar is installed
Table Name (is required)	Table identified by name.
Outer Key (is required)	The outer key of the value to remove
Inner Key (is required)	The inner key of the value to remove
Fields	Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Value (is required)	The value to remove from the reference table. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.
Domain ID	This allows the domain id for the value to be specified. If null, the shared domain will be used.

Outputs	Description
values (values)	The results of the API call

IBM QRadar/Ariel Search method

Creates a new Ariel search as specified by the Ariel Query Language (AQL) query expression. Searches are executed asynchronously. A reference to the search ID is returned and should be used in subsequent API calls to determine the status of the search and retrieve the results once it is complete. This endpoint only accepts SELECT query expressions.

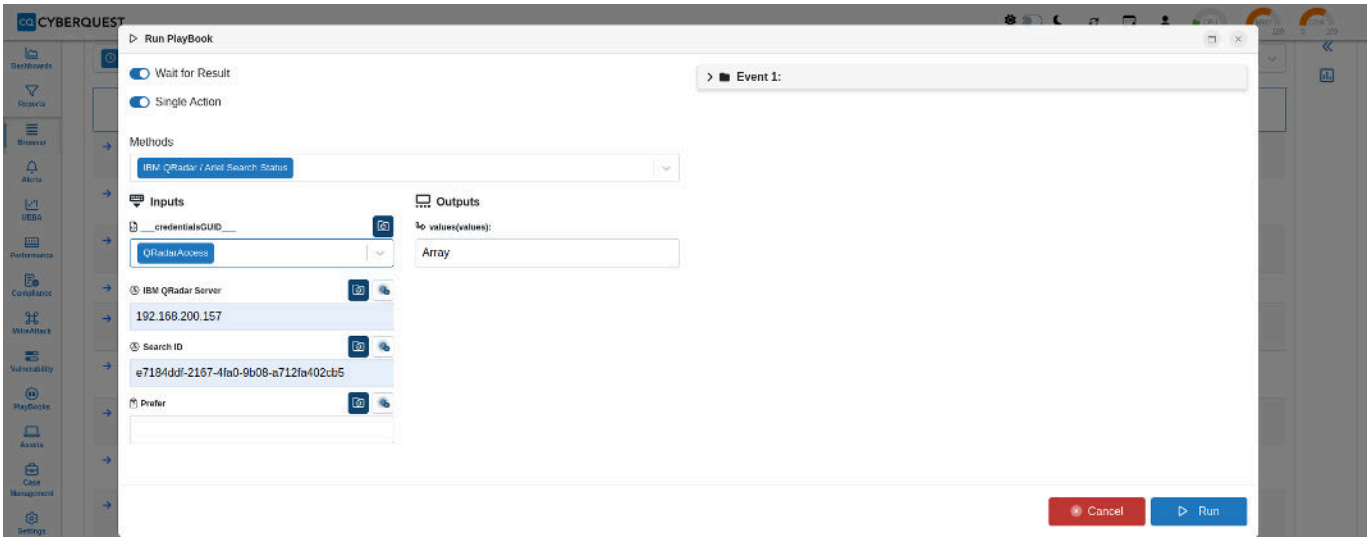


Inputs	Description
credentialsGUID (is required)	
IBM QRadar Server (is required)	The server where the IBM QRadar is installed
Query Expression (is required)	The AQL query to execute. Mutually exclusive with saved_search_id

Outputs	Description
values (values)	The results of the API call

IBM QRadar/Ariel Search Status method

Retrieve status information for a search, based on the search ID parameter. The same informational fields are returned regardless of whether the search is in progress or is complete.

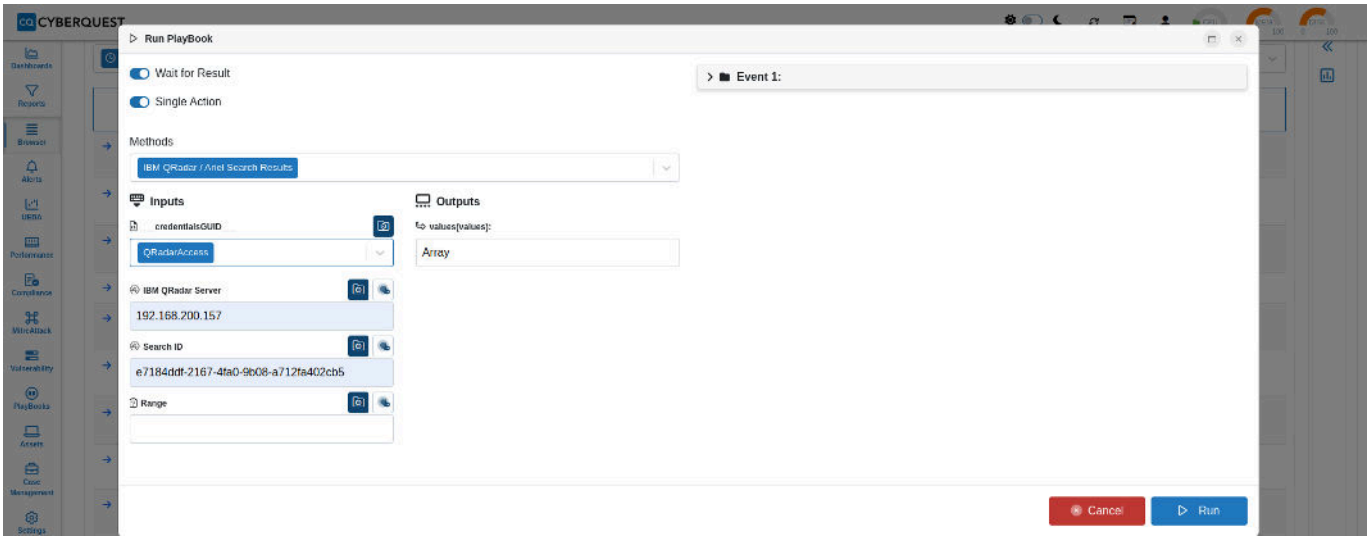


Inputs	Description
credentialsGUID (is required)	
IBM QRadar Server (is required)	The server where the IBM QRadar is installed
Search ID (is required)	The ID of the search criteria for the returned results.
Prefer	Specify wait=N where N is number of seconds to wait for COMPLETED status of the search.

Outputs	Description
values (values)	The results of the API call

IBM QRadar/Ariel Search Results method

Retrieves search results in the requested format.Retrieve the results of the Ariel search that is identified by the search ID. The Accepts request header indicates the format of the result. The formats are RFC compliant and can be JSON, CSV, XML, or tabular text.By default, all query result records are returned. To restrict the results to a contiguous subset of the records, you can supply a Range header to specify the inclusive range of records to be returned.This end-point works with query results that are generated by AQL query expressions. This endpoint might not work as expected for results that are generated by other means. Search results might not be retrievable for searches that are created on the Console.The response samples are for the following query: Select sourceIP, destinationIP from events.

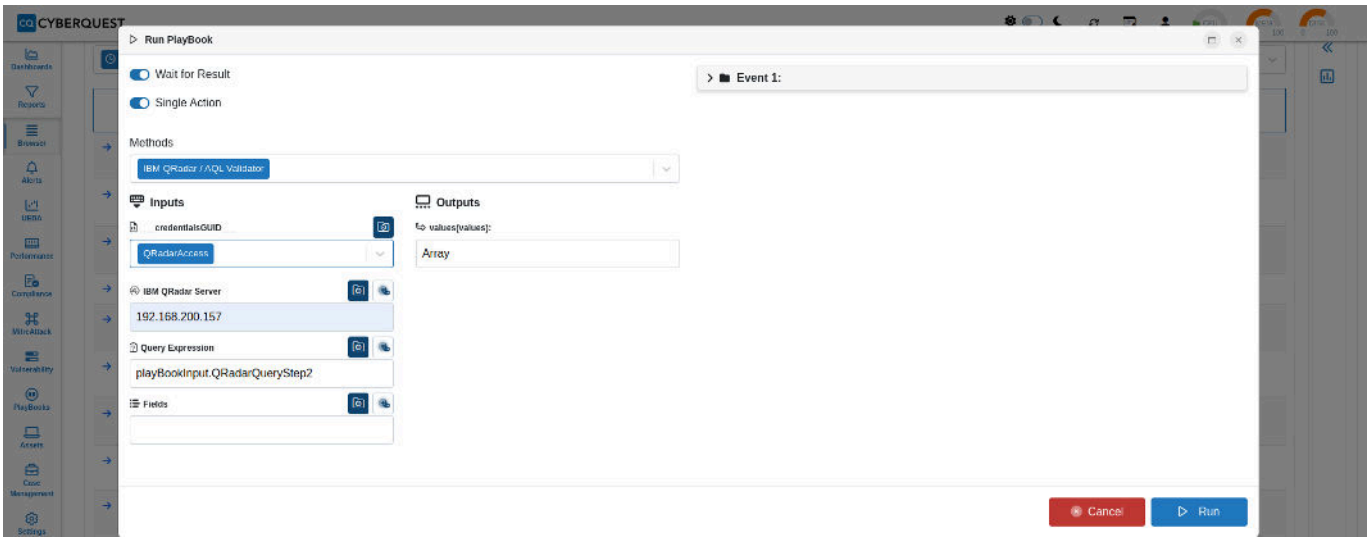


Inputs	Description
credentialsGUID (is required)	
IBM QRadar Server (is required)	The server where the IBM QRadar is installed
Search ID (is required)	The ID of the search criteria for the returned results.
Range	Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.

Outputs	Description
values (values)	The results of the API call

IBM QRadar/AQL Validator method

Creates a new Ariel search as specified by the Ariel Query Language (AQL) query expression. Searches are executed asynchronously. A reference to the search ID is returned and should be used in subsequent API calls to determine the status of the search and retrieve the results once it is complete. This endpoint only accepts SELECT query expressions.



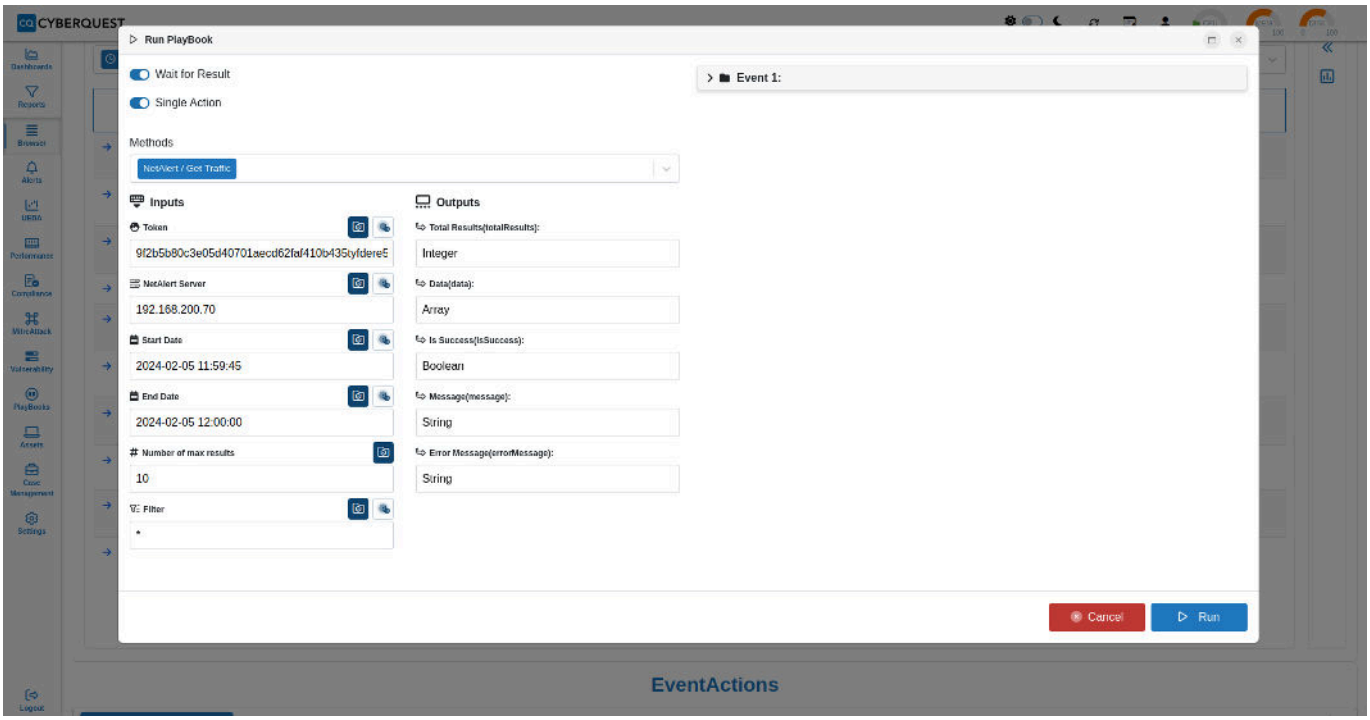
Inputs	Description
credentialsGUID (is required)	
IBM QRadar Server (is required)	The server where the IBM QRadar is installed
Query Expression (is required)	The AQL query to execute. Mutually exclusive with saved_search_id
Fields	- Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Outputs	Description
values (values)	The results of the API call

NETALERT

NetAlert/Get Traffic method

This action help you to extract traffic information.

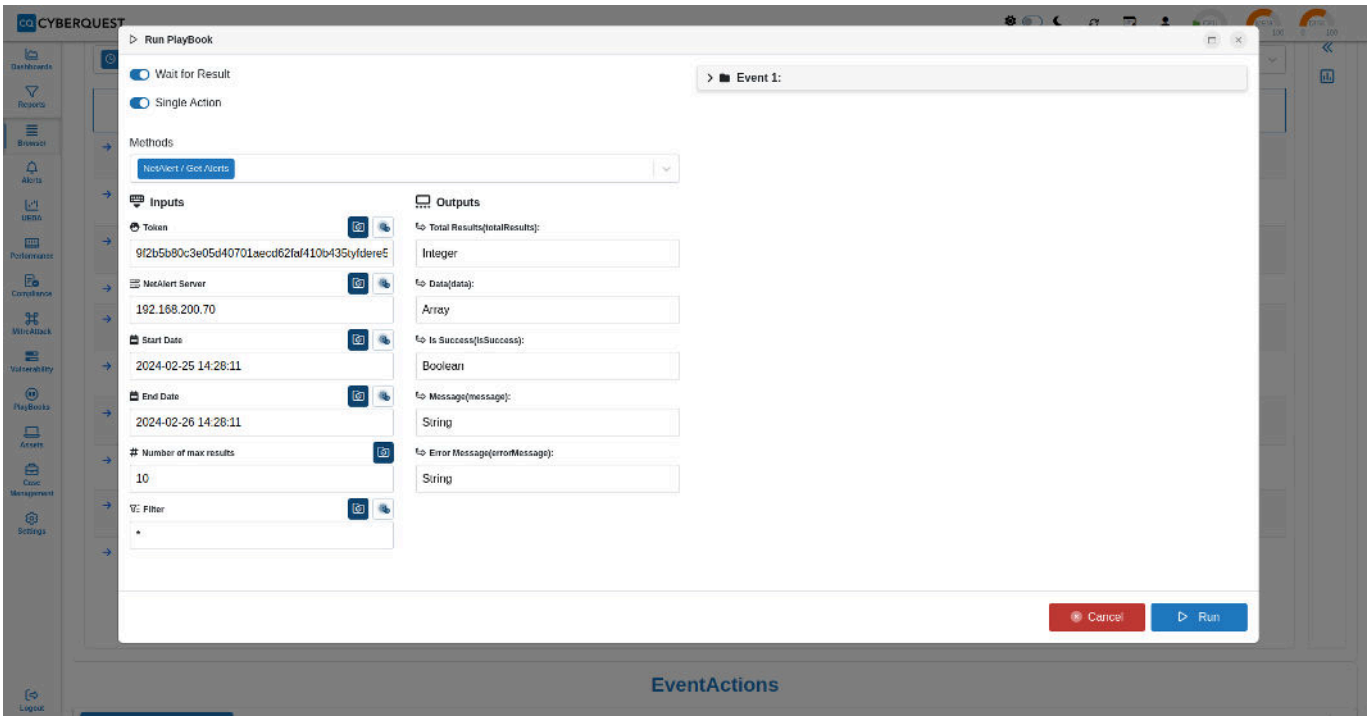


Inputs	Description
Token (is required)	To use this api you need an API Key
NetAlert Server (is required)	IP of the server where NetAlert is installed
Start Date (is required)	The start time of the search
End Date (is required)	The end time of the search
Number of max results	The maximum number of elements which resulted from the api called you want to return
Filter	The OpenSearch filter, a query string query for data filtering

Outputs	Description
Total Results (totalResults)	The total number of reports
Data (data)	Reports from NetAlert based on search filter
Is Success (isSuccess)	True if the API call was successful, otherwise false
Message (message)	Additional details
Error Message (errorMessage)	Details of the error that occurred during the API call

NetAlert/Get Alerts method

This action help you to extract alerts information.

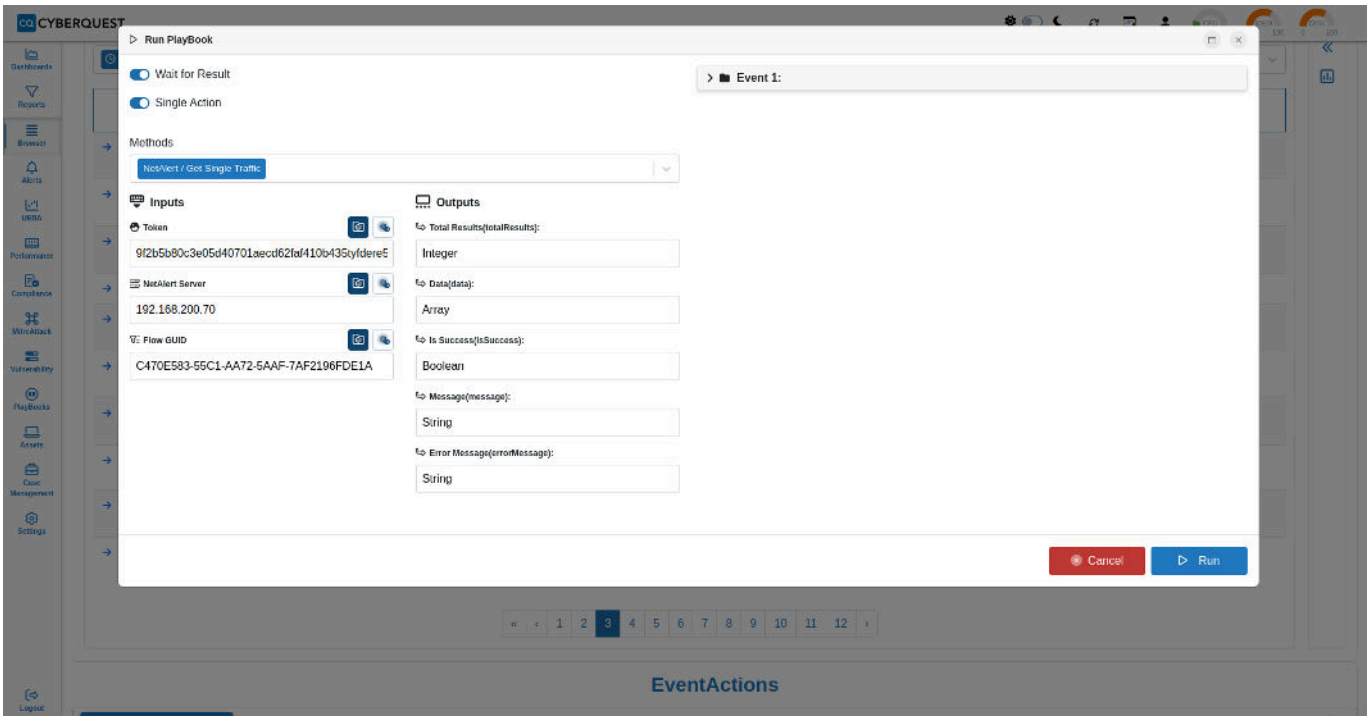


Inputs	Description
Token (is required)	To use this api you need an API Key
NetAlert Server (is required)	IP of the server where NetAlert is installed
Start Date (is required)	The start time of the search
End Date (is required)	The end time of the search
Number of max results	The maximum number of elements which resulted from the api called you want to return
Filter	The OpenSearch filter, a query string query for data filtering

Outputs	Description
Total Results (totalResults)	The total number of reports
Data (data)	Reports from NetAlert based on search filter
Is Success (isSuccess)	True if the API call was successful, otherwise false
Message (message)	Additional details
Error Message (errorMessage)	Details of the error that occurred during the API call

NetAlert/Get Single Traffic method

This action help you to extract single traffic information.

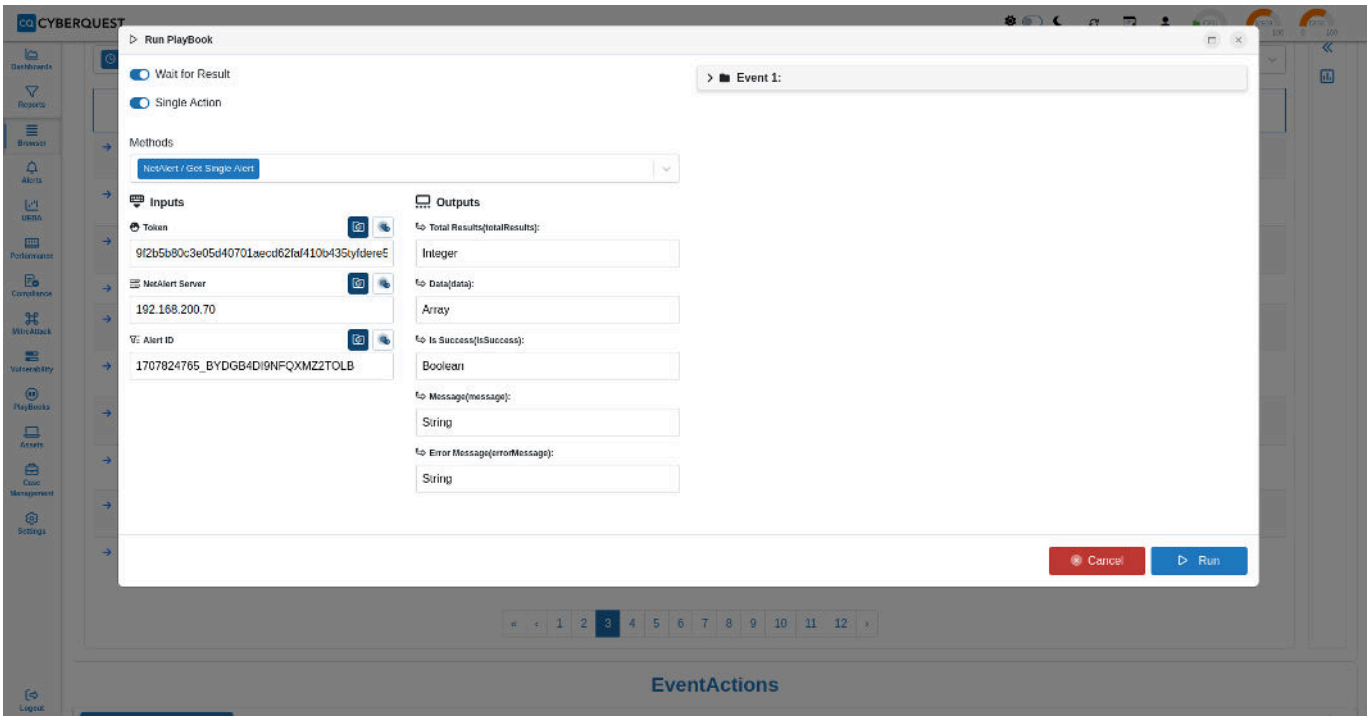


Inputs	Description
Token (is required)	To use this api you need an API Key
NetAlert Server (is required)	IP of the server where NetAlert is installed
Flow GUID (is required)	A unique identifier which is given to all traffic flows (traffic which obeys a request/response structure).

Outputs	Description
Total Results (totalResults)	The total number of reports
Data (data)	Reports from NetAlert based on search filter
Is Success (isSuccess)	True if the API call was successful, otherwise false
Message (message)	Additional details
Error Message (errorMessage)	Details of the error that occurred during the API call

NetAlert/Get Single Alert method

This action help you to extract single alert information.

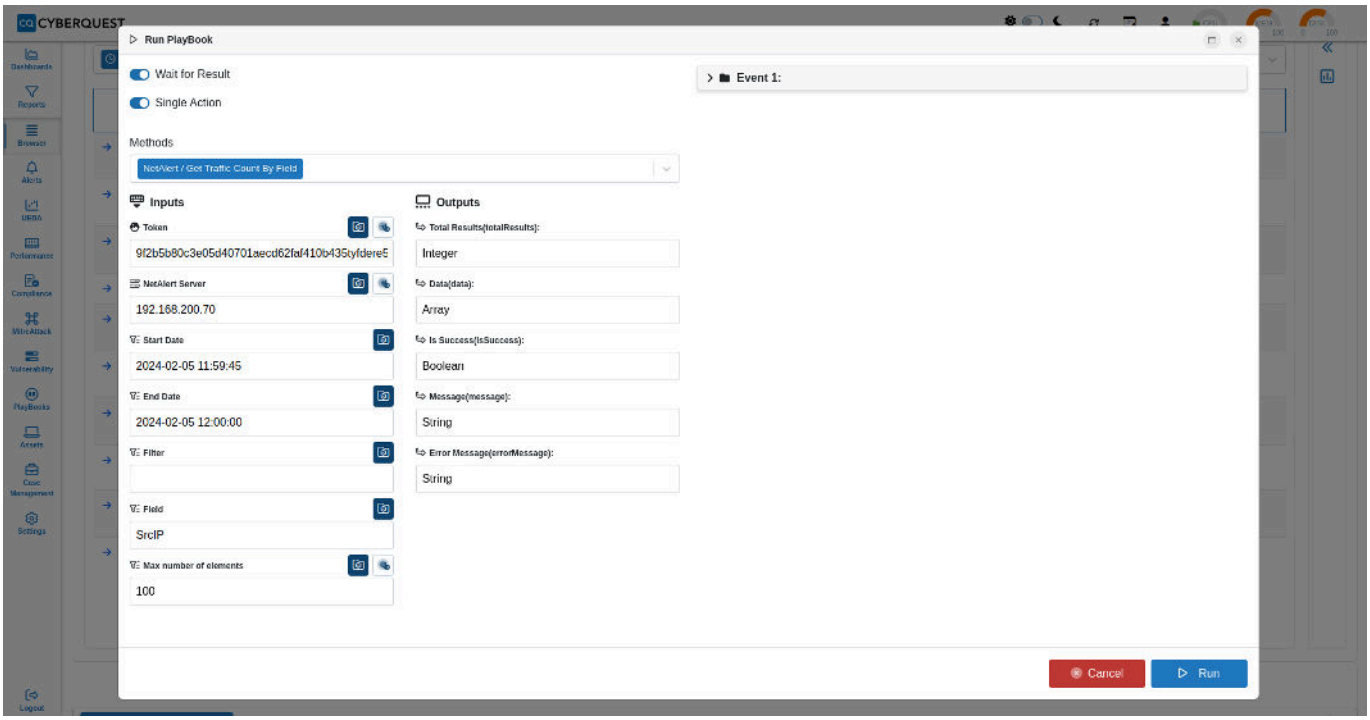


Inputs	Description
Token (is required)	To use this api you need an API Key
NetAlert Server (is required)	IP of the server where NetAlert is installed
Alert ID (is required)	A unique identifier given in the DB for the alert.

Outputs	Description
Total Results (totalResults)	The total number of reports
Data (data)	Reports from NetAlert based on search filter
Is Success (isSuccess)	True if the API call was successful, otherwise false
Message (message)	Additional details
Error Message (errorMessage)	Details of the error that occurred during the API call

NetAlert/Get Traffic Count By Field method

Get traffic count with the help of the field parameter.

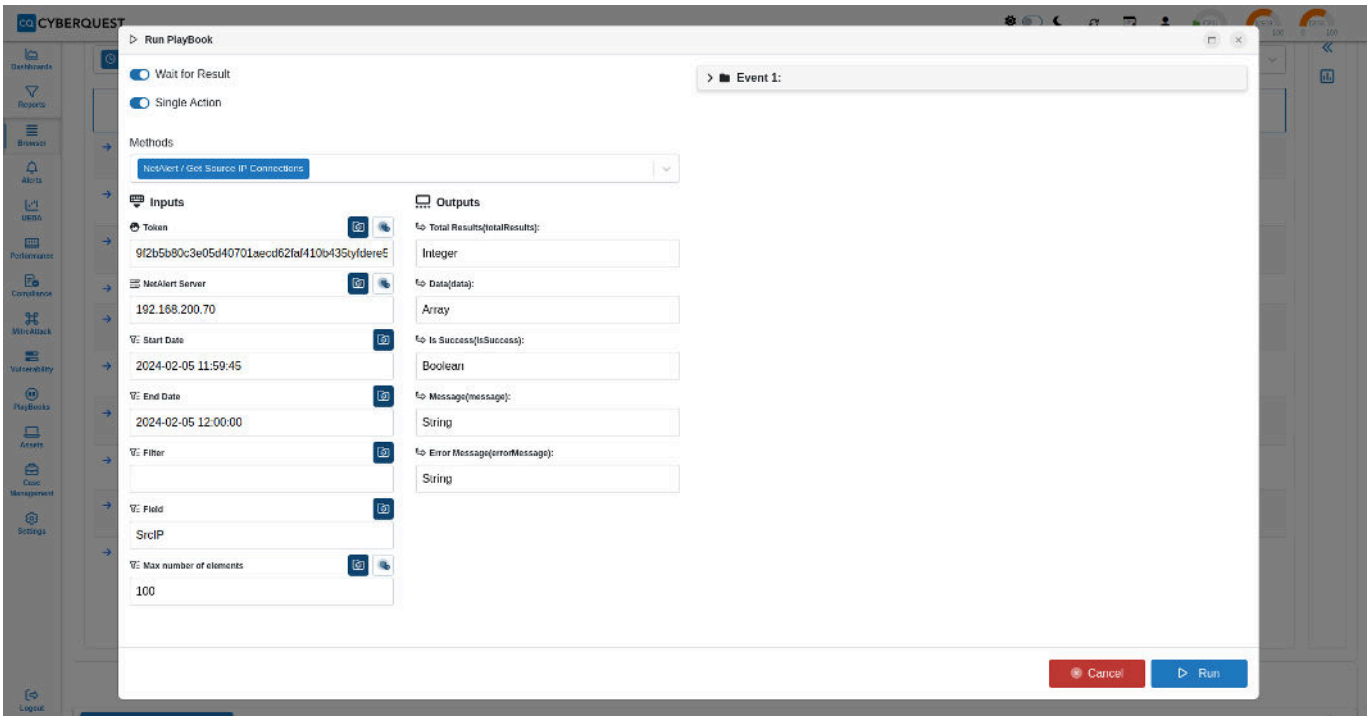


Inputs	Description
Token (is required)	To use this api you need an API Key
NetAlert Server (is required)	IP of the server where NetAlert is installed
Start Date (is required)	The start time of the search
End Date (is required)	The end time of the search
Filter	The OpenSearch filter, a query string query for data filtering
Field (is required)	The field you want to search by
Max number of elements	The maximum number of elements which resulted from the api called you want to return

Outputs	Description
Total Results (totalResults)	The total number of reports
Data (data)	Reports from NetAlert based on search filter
Is Success (isSuccess)	True if the API call was successful, otherwise false
Message (message)	Additional details
Error Message (errorMessage)	Details of the error that occurred during the API call

NetAlert/Get Source IP Connections method

Get Source IP Connections.

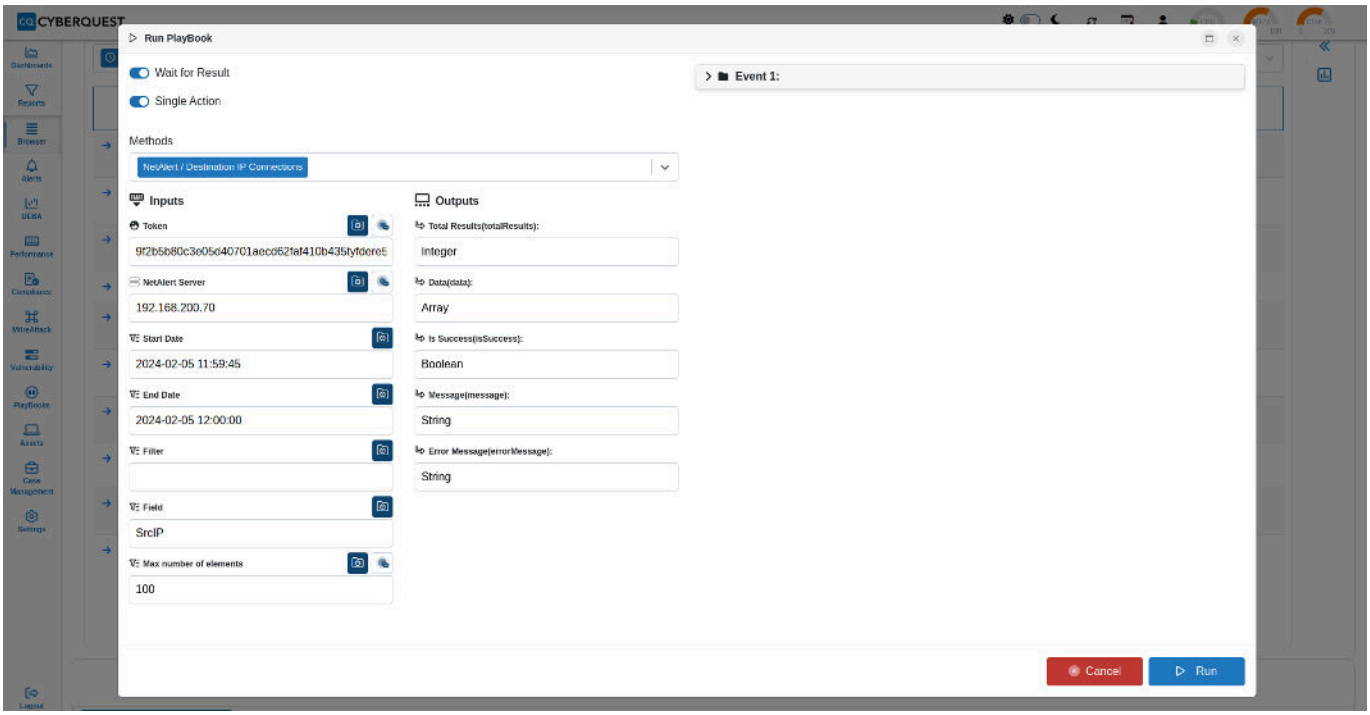


Inputs	Description
Token (is required)	To use this api you need an API Key
NetAlert Server (is required)	IP of the server where NetAlert is installed
Start Date (is required)	The start time of the search
End Date (is required)	The end time of the search
Filter	The OpenSearch filter, a query string query for data filtering
Field (is required)	The field you want to search by
Max number of elements	The maximum number of elements which resulted from the api called you want to return

Outputs	Description
Total Results (totalResults)	The total number of reports
Data (data)	Reports from NetAlert based on search filter
Is Success (isSuccess)	True if the API call was successful, otherwise false
Message (message)	Additional details
Error Message (errorMessage)	Details of the error that occurred during the API call

NetAlert/Destination IP Connections method

Get Destination IP Connections.

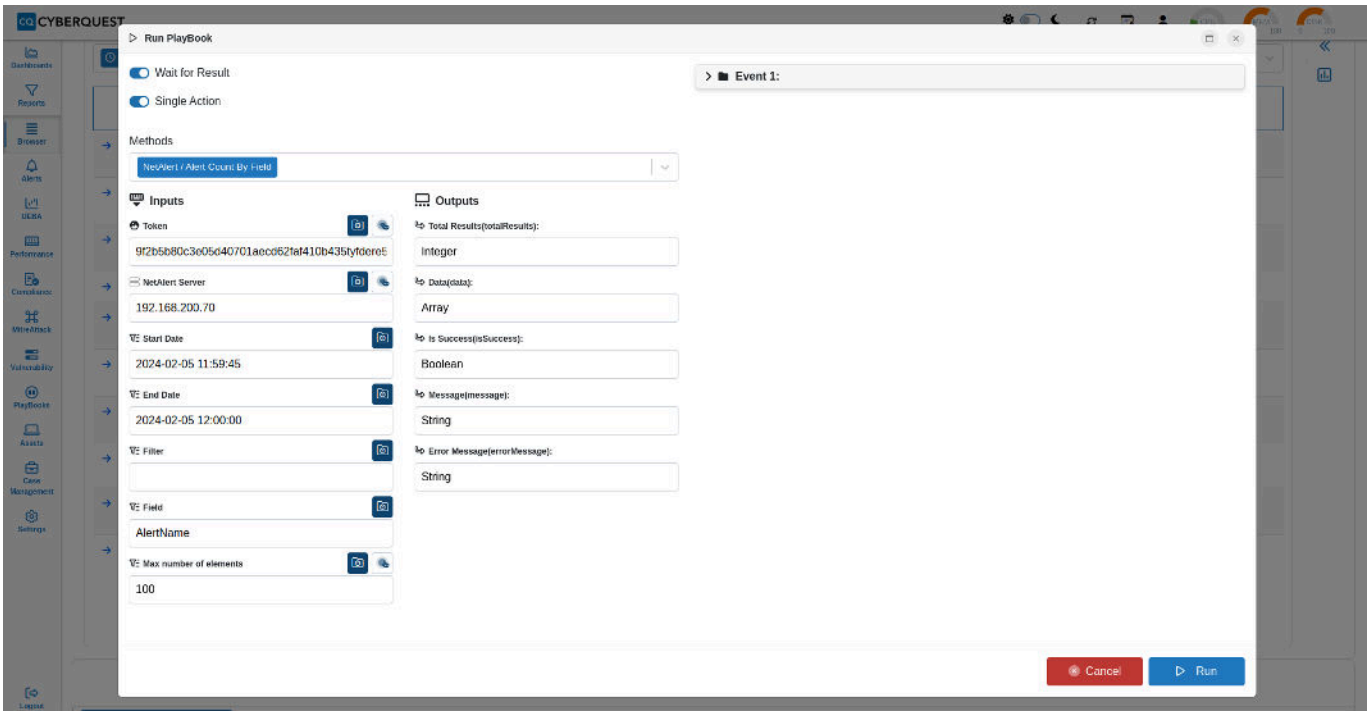


Inputs	Description
Token (is required)	To use this api you need an API Key
NetAlert Server (is required)	IP of the server where NetAlert is installed
Start Date (is required)	The start time of the search
End Date (is required)	The end time of the search
Filter	The OpenSearch filter, a query string query for data filtering
Field (is required)	The field you want to search by
Max number of elements	The maximum number of elements which resulted from the api called you want to return

Outputs	Description
Total Results (totalResults)	The total number of reports
Data (data)	Reports from NetAlert based on search filter
Is Success (isSuccess)	True if the API call was successful, otherwise false
Message (message)	Additional details
Error Message (errorMessage)	Details of the error that occurred during the API call

NetAlert/Alert Count By Field method

Get Alerts Count By a Field IP.



Inputs	Description
Token (is required)	To use this api you need an API Key
NetAlert Server (is required)	IP of the server where NetAlert is installed
Start Date (is required)	The start time of the search
End Date (is required)	The end time of the search
Filter	The OpenSearch filter, a query string query for data filtering
Field (is required)	The field you want to search by
Max number of elements	The maximum number of elements which resulted from the api called you want to return

Outputs	Description
Total Results (totalResults)	The total number of reports
Data (data)	Reports from NetAlert based on search filter
Is Success (isSuccess)	True if the API call was successful, otherwise false
Message (message)	Additional details
Error Message (errorMessage)	Details of the error that occurred during the API call

Tenable Nessus

Tenable Nessus/Create Scan

Creates a scan configuration.

Inputs	Description
Access Key (is required)	To use the ThreatBook API, you must have an API key.
Secret Key (is required)	The IP which is investigated
UUID (is required)	The UUID for the Tenable-provided scan template to use
Settings (is required)	The settings of the new scan
Credentials	The settings of the new scan

Outputs	Description
Scan (scan)	The result of the API call

Tenable Nessus/Launch Scan

Launches a scan.

Inputs	Description
Access Key (is required)	To use the ThreatBook API, you must have an API key.
Secret Key (is required)	The IP which is investigated
Scan ID (is required)	The unique identifier for the scan you want to launch. This identifier can be either the scans.schedule_uuid or the scans.id
Alt targets	If you include this parameter, Tenable Vulnerability Management scans these targets instead of the default. Value can be an array where each index is a target, or an array with a single index of comma-separated targets.
Rollover	The settings of the new scan

Outputs	Description
scan_uuid (scan_uuid)	The UUID of the scan launched.

Tenable Nessus/Export Scan

Export the specified scan.

Inputs	Description
Access Key (is required)	To use the ThreatBook API, you must have an API key.
Secret Key (is required)	The IP which is investigated
Scan ID (is required)	The unique identifier for the scan you want to launch. This identifier can be either the scans.schedule_uuid or the scans.id
History ID	The unique identifier of the historical data that you want Tenable Vulnerability Management to export.
Asset ID	The settings of the new scan

Outputs	Description
file (file)	The file ID of the export scan
temp_token(temp_token)	Temporary Token of the export scan

Tenable Nessus/Check Scan Export Status

Check the file status of an exported scan.

Inputs	Description
Access Key (is required)	To use the ThreatBook API, you must have an API key.
Secret Key (is required)	The IP which is investigated
Scan ID (is required)	The unique identifier for the scan you want to launch. This identifier can be either the scans.schedule_uuid or the scans.id
File ID (is required)	The ID of the file to download
Asset ID	The settings of the new scan

Outputs	Description
file (file)	The file ID of the Check Scan Export Status
temp_token(temp_token)	Temporary Token of the Check Scan Export Status

Tenable Nessus/Download Exported Scan

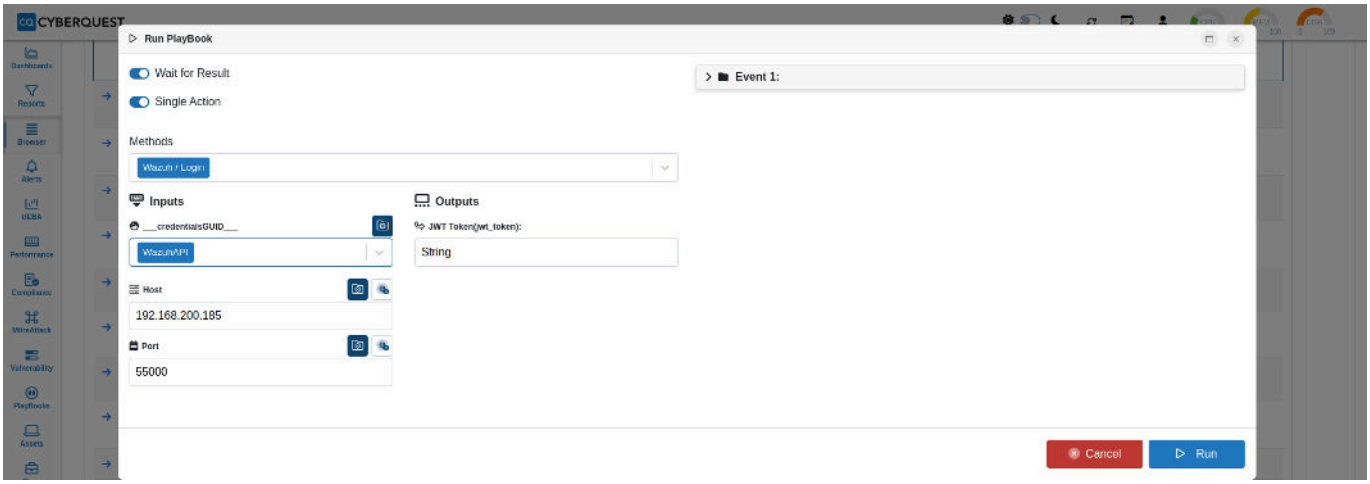
Download an exported scan.

Inputs	Description
Access Key (is required)	To use the ThreatBook API, you must have an API key.
Secret Key (is required)	The IP which is investigated
Scan ID (is required)	The unique identifier for the scan you want to launch. This identifier can be either the scans.schedule_uuid or the scans.id
File ID	The ID of the file to download

Wazuh

Wazuh/Login method

Use this method to generate JWT Token which will be used as a method of login for other APIs from Wazuh.

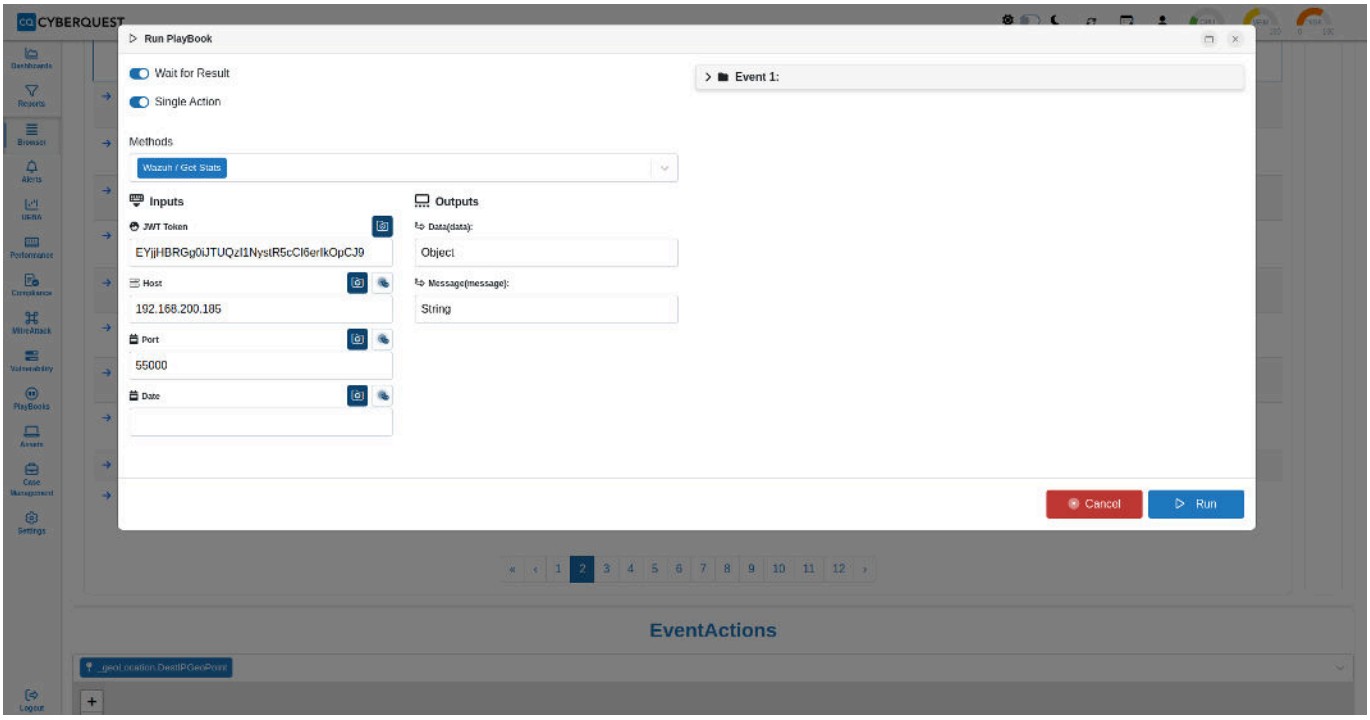


Inputs	Description
credentialsGUID (is required)	The credentials of the Wazuh Server
Host (is required)	IP of the server where Wazuh is installed
Port (is required)	The port used by the API

Outputs	Description
JWT Token (jwt_token)	The login token

Wazuh/Get Stats method

Return Wazuh statistical information for the current or specified date.

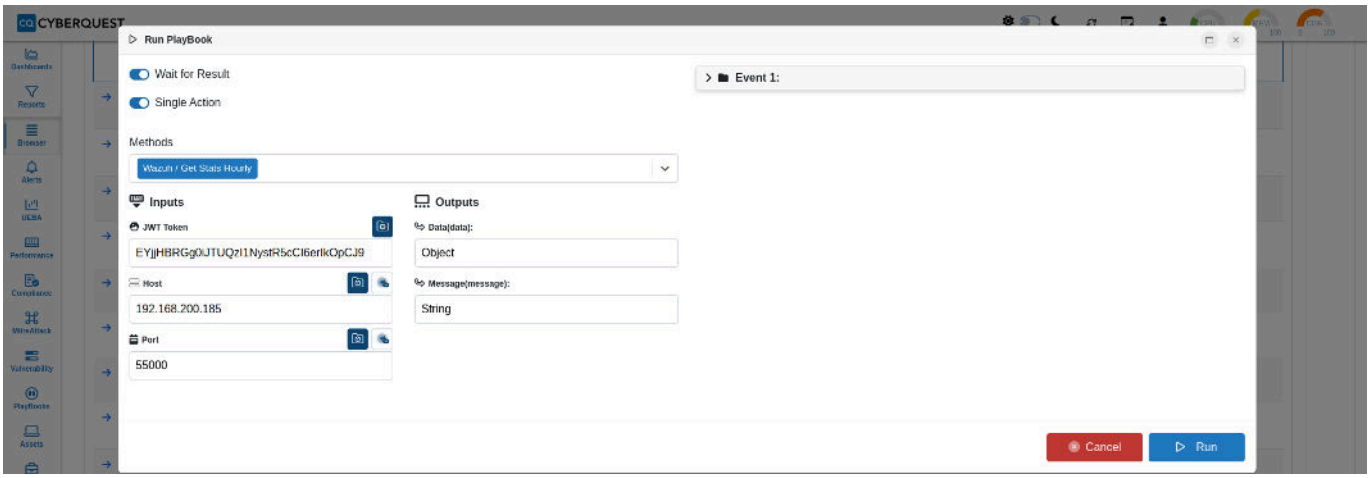


Inputs	Description
JWT Token (is required)	The token that was generated from login method
Host (is required)	IP of the server where Wazuh is installed
Port (is required)	The port used by the API
Date	Date to obtain statistical information from. Format YYYY-MM-DD

Outputs	Description
Data (data)	The results of the API call
Message (message)	Human readable description to explain the result of the request

Wazuh/Get Stats Hourly method

Return Wazuh statistical information per hour. Each number in the averages field represents the average of alerts per hour for that specific day.

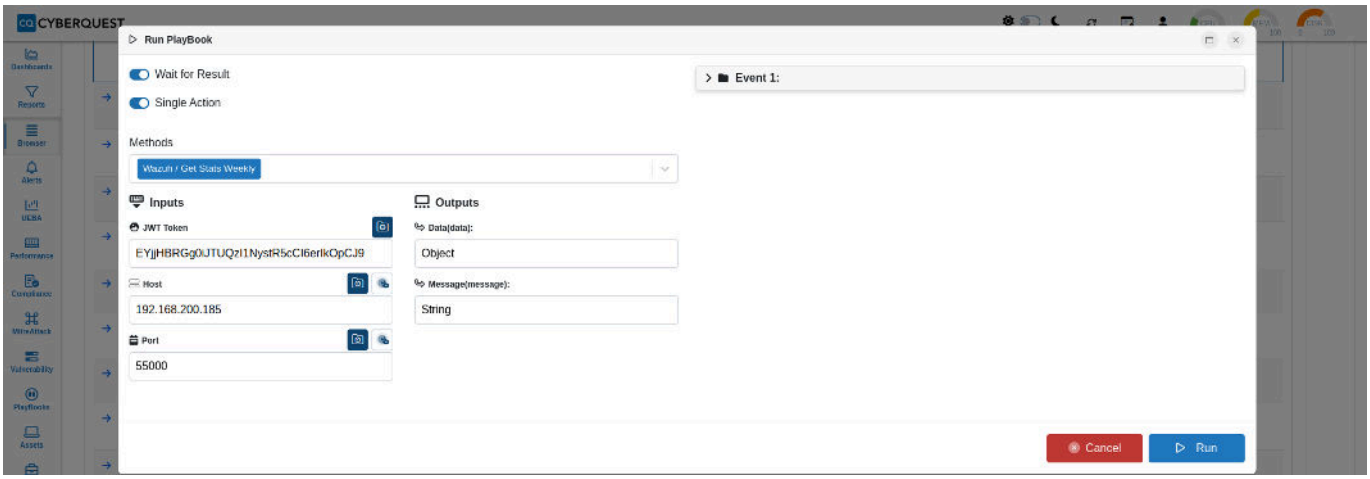


Inputs	Description
JWT Token (is required)	The token that was generated from login method
Host (is required)	IP of the server where Wazuh is installed
Port (is required)	The port used by the API

Outputs	Description
Data (data)	The results of the API call
Message (message)	Human readable description to explain the result of the request

Wazuh/Get Stats Weekly method

Return Wazuh statistical information per week. Each number in the averages field represents the average of alerts per hour for that specific day.

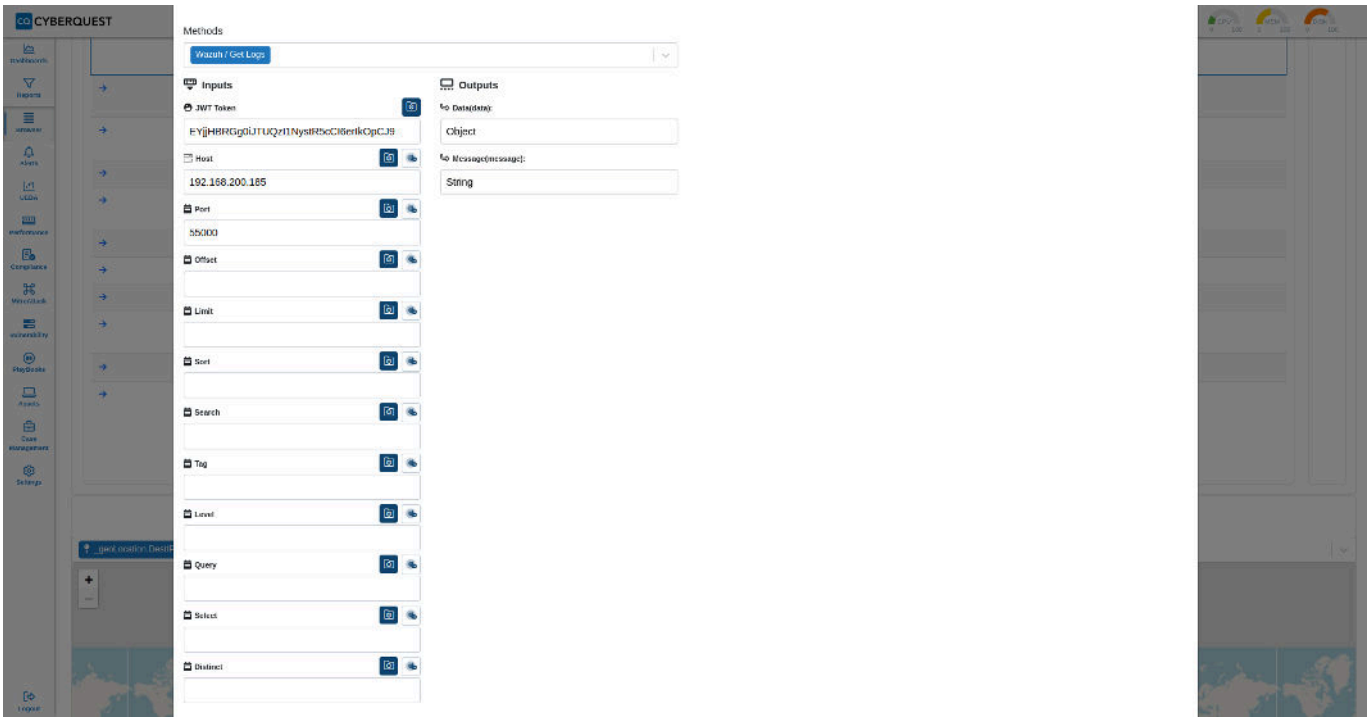


Inputs	Description
JWT Token (is required)	The token that was generated from login method
Host (is required)	IP of the server where Wazuh is installed
Port (is required)	The port used by the API

Outputs	Description
Data (data)	The results of the API call
Message (message)	Human readable description to explain the result of the request

Wazuh/Get Logs method

Return the last 2000 wazuh log entries.

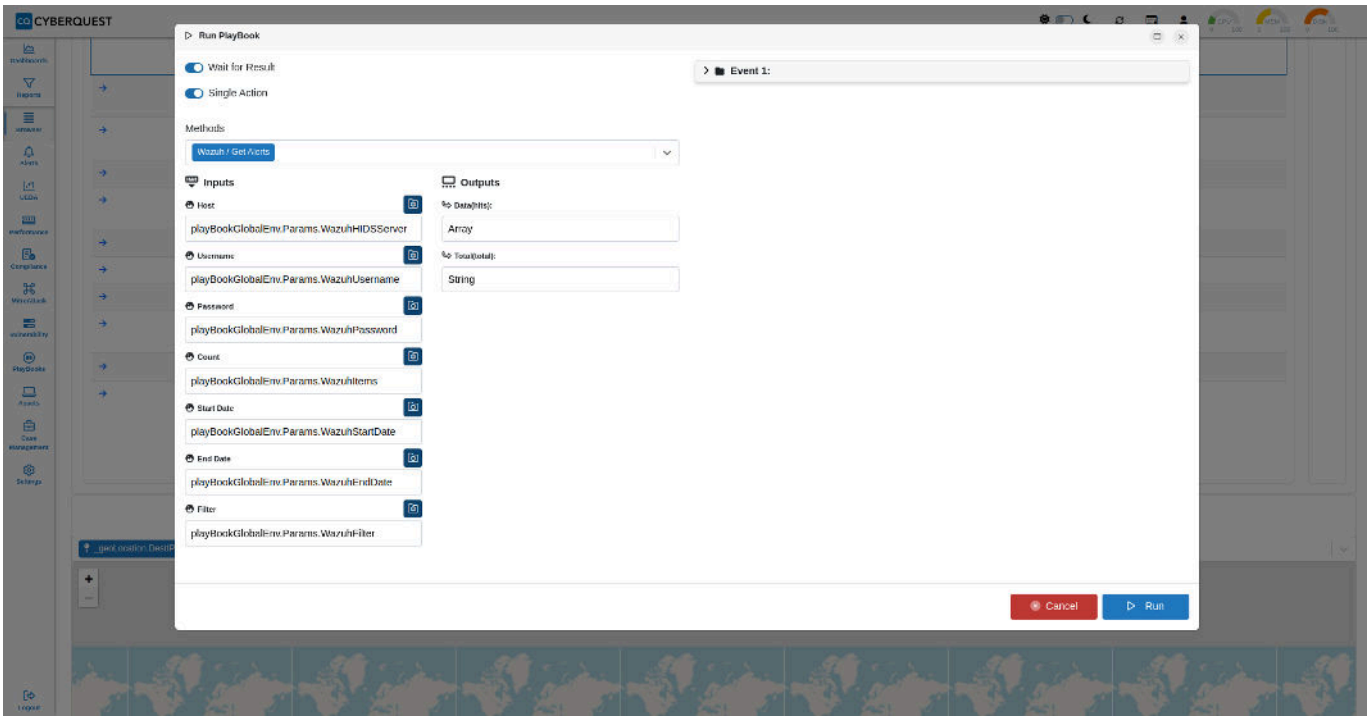


Inputs	Description
JWT Token (is required)	The token that was generated from login method
Host (is required)	IP of the server where Wazuh is installed
Port (is required)	The port used by the API
Offset	First element to return in the collection
Limit	Maximum number of lines to return
Sort	Sort the collection by a field or fields (separated by comma). Use +/- at the beggining to list in ascending or descending order. Use . for nested fields. For example, {field1: field2} may be selected with field1.field2
Search	Look for elements containing the specified string. To obtain a complementary search, use - at the beginning
Tag	Wazuh component that logged the event
Level	Enum: critical, debug, debug2, error, info, warning
Query	Query to filter results by. For example query= status=active
Select	Select which fields to return (separated by comma). Use . for nested fields. For example, {field1: field2} may be selected with field1.field2
Distinct	Look for distinct values

Outputs	Description
Data (data)	The results of the API call
Message (message)	Human readable description to explain the result of the request

Wazuh/Get Alerts method

Get Alerts from Wazuh.

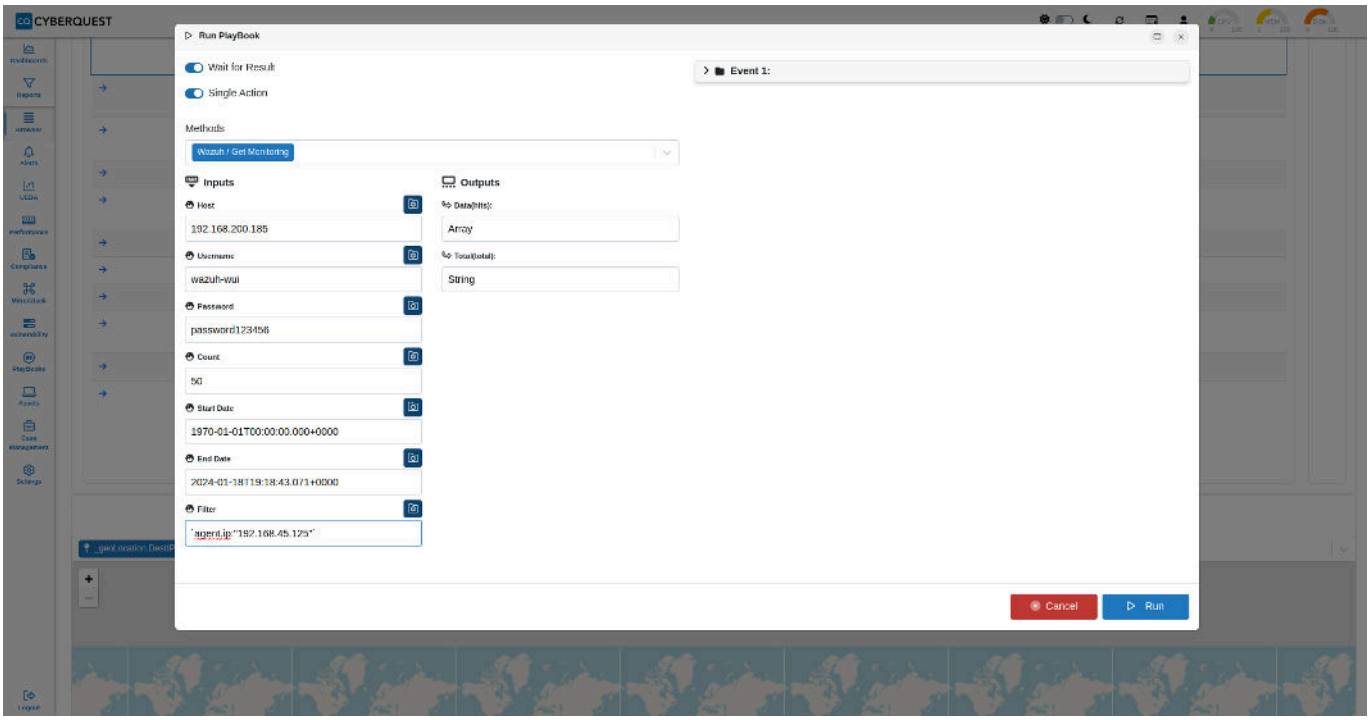


Inputs	Description
Host (is required)	IP of the server where Wazuh is installed
Username (is required)	The Username which is used to login in Wazuh OpenSearch
Password (is required)	The Password which is used to login in Wazuh OpenSearch
Count (is required)	The number of alerts you want to receive from OpenSearch
Start Date (is required)	The start time of the search
End Date (is required)	The end time of the search
Filter (is required)	The OpenSearch filter, a query string query for data filtering

Outputs	Description
Data (hits)	The results of the API call
Total (total)	The total number of alerts

Wazuh/Get Monitoring method

Get Monitoring logs from Wazuh.

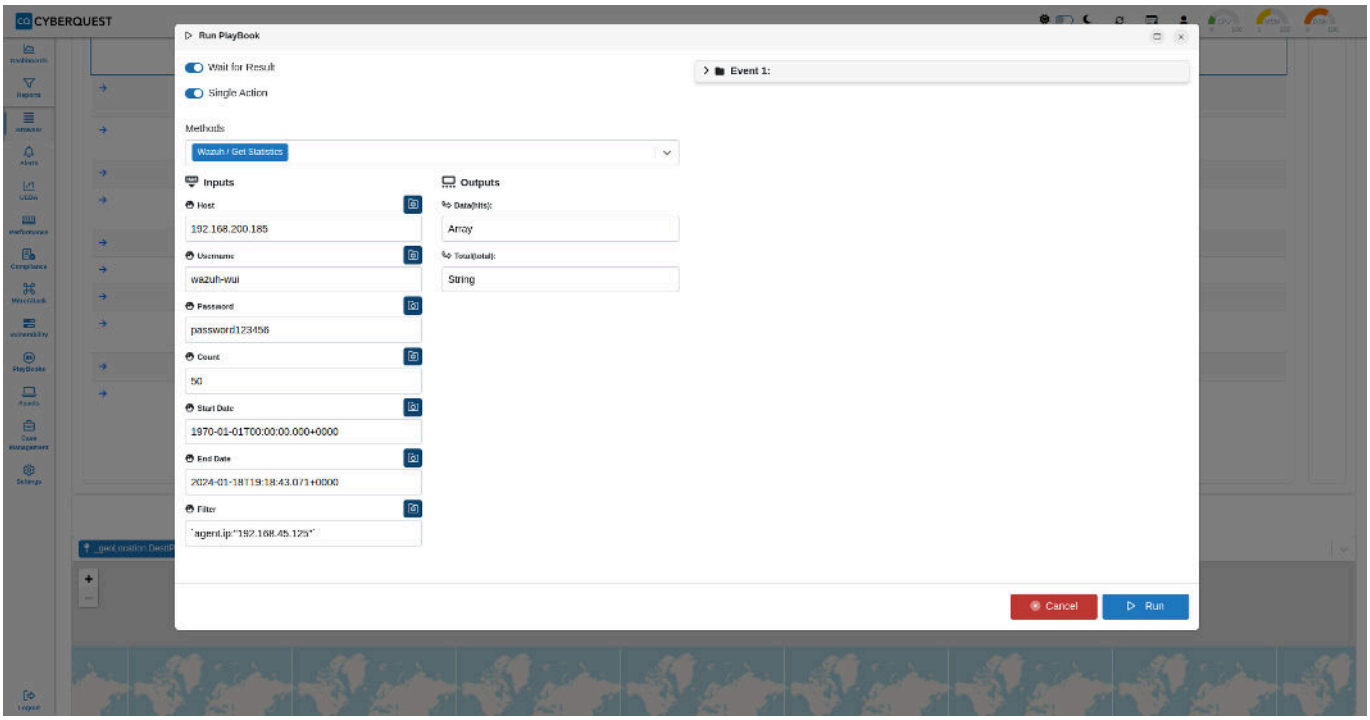


Inputs	Description
Host (is required)	IP of the server where Wazuh is installed
Username (is required)	The Username which is used to login in Wazuh OpenSearch
Password (is required)	The Password which is used to login in Wazuh OpenSearch
Count (is required)	The number of alerts you want to receive from OpenSearch
Start Date (is required)	The start time of the search
End Date (is required)	The end time of the search
Filter (is required)	The OpenSearch filter, a query string query for data filtering

Outputs	Description
Data (hits)	The results of the API call
Total (total)	The total number of alerts

Wazuh/Get Statistics method

Get Statistics logs from Wazuh.

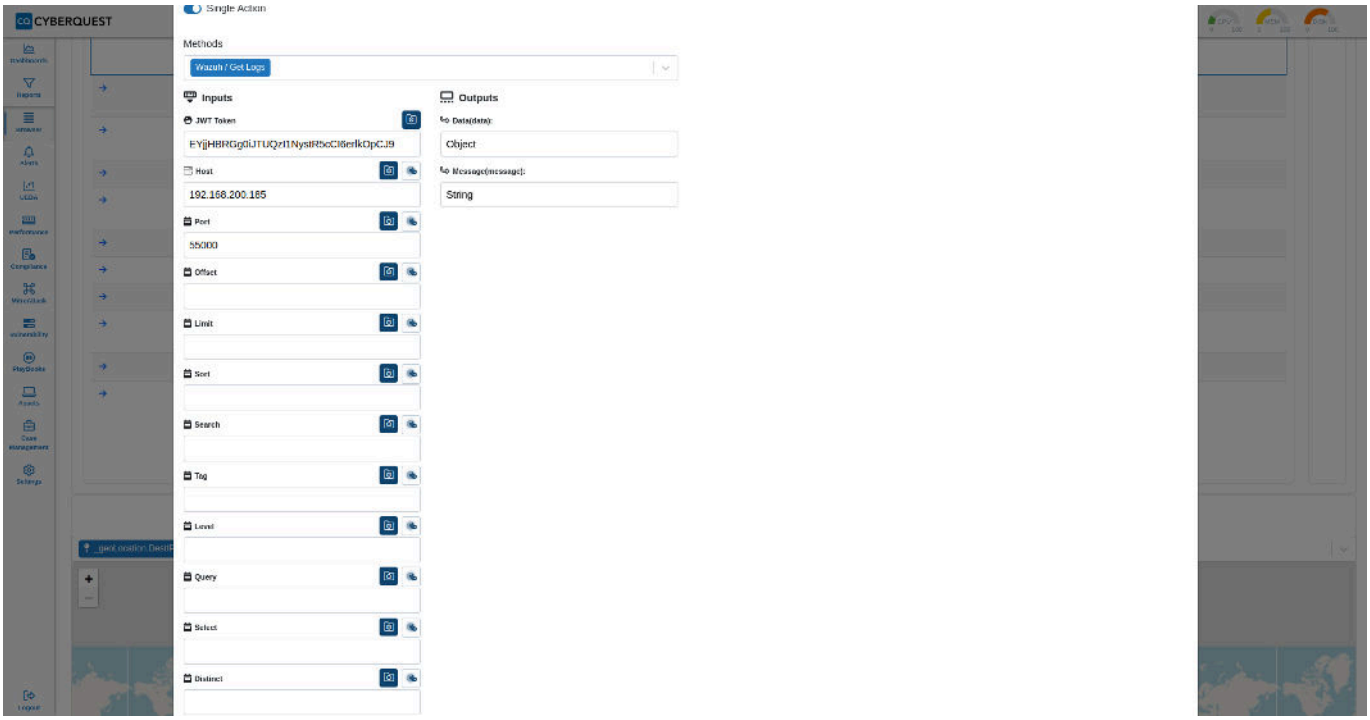


Inputs	Description
Host (is required)	IP of the server where Wazuh is installed
Username (is required)	The Username which is used to login in Wazuh OpenSearch
Password (is required)	The Password which is used to login in Wazuh OpenSearch
Count (is required)	The number of alerts you want to receive from OpenSearch
Start Date (is required)	The start time of the search
End Date (is required)	The end time of the search
Filter (is required)	The OpenSearch filter, a query string query for data filtering

Outputs	Description
Data (hits)	The results of the API call
Total (total)	The total number of alerts

Wazuh/Get Logs Summary method

Return a summary of the last 2000 wazuh log entries.

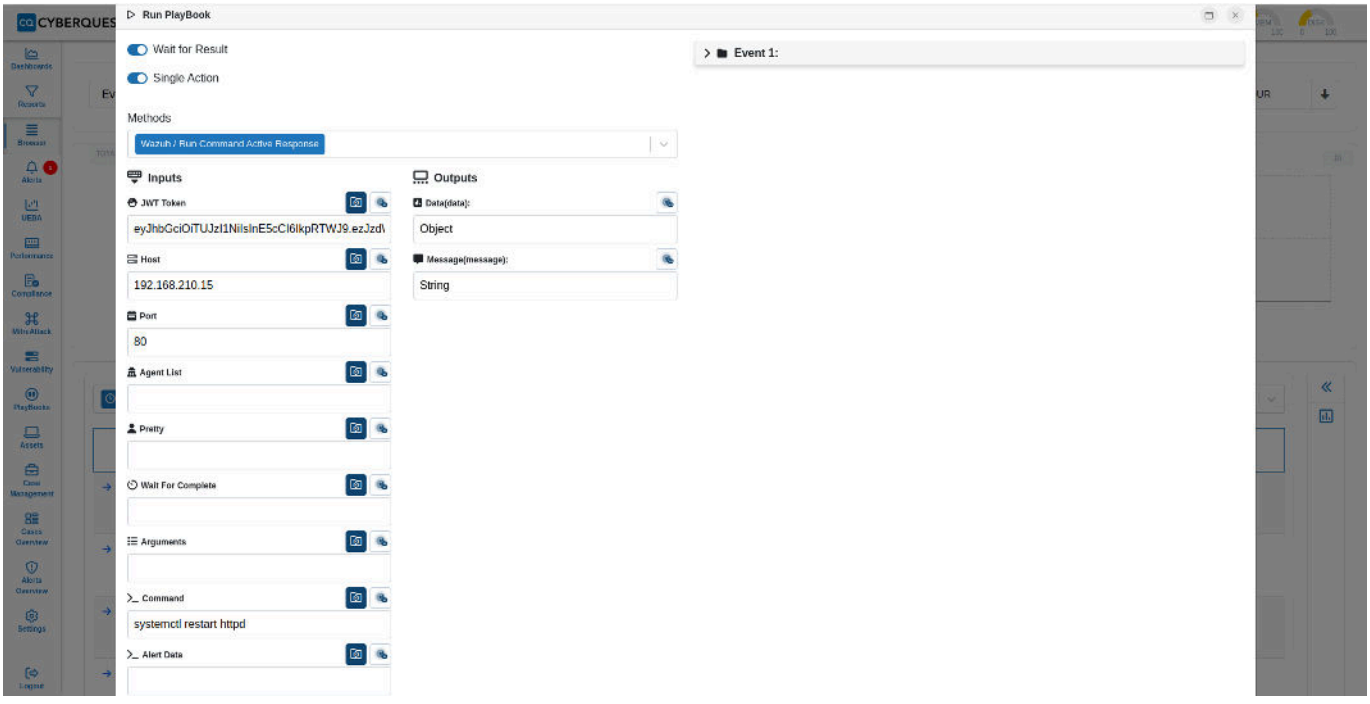


Inputs	Description
JWT Token (is required)	The token that was generated from login method
Host (is required)	IP of the server where Wazuh is installed
Port (is required)	The port used by the API

Outputs	Description
Data (data)	The results of the API call
Message (message)	Human readable description to explain the result of the request

Wazuh/Run Command Active Response

Run an Active Response command on all agents or a list of them.



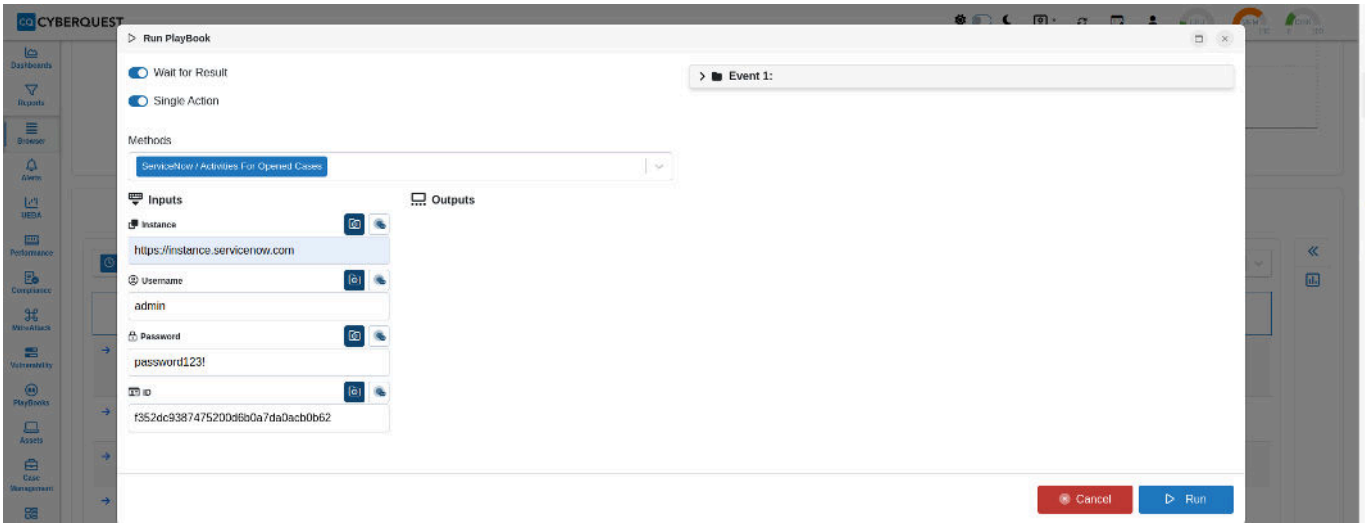
Inputs	Description
JWT Token (is required)	The token that was generated from login method
Host (is required)	IP of the server where Wazuh is installed
Port (is required)	The port used by the API
Agent List	List of agent IDs (separated by comma), all agents selected by default if not specified
Pretty	Show results in human-readable format
Wait For Complete	Disable timeout response
Arguments	Command arguments
Command (is required)	Command running in the agent. If this value starts with !, then it refers to a script name instead of a command name
Alert Data	Alert data depending on the active response command executed

Outputs	Description
Data (data)	The results of the API call
Message (message)	Human readable description to explain the result of the request

ServiceNow

ServiceNow/Activities For Opened Cases

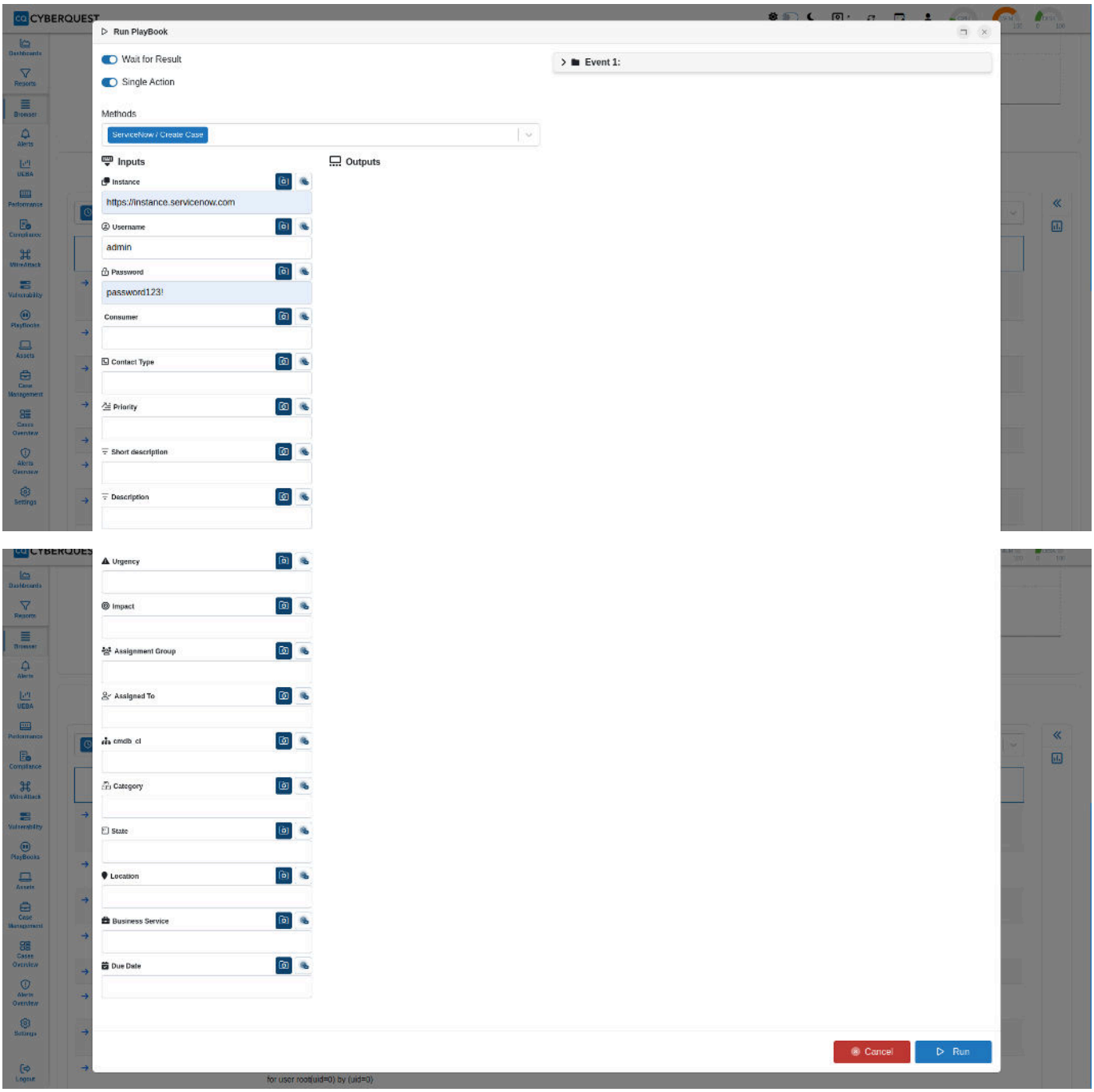
The list of activities opened for a case.



Inputs	Description
Instance (is required)	The subdomain created using ServiceNow, for example: nextgensoftware
Username (is required)	To use this API you must have an account valid account on ServiceNow. Use the username used to login in ServiNow Interface
Password (is required)	To use this API you must have an account valid account on ServiceNow. Use the password used to login in ServiNow Interface
ID (is required)	The ID of the Opened Case you want to get the activity list

ServiceNow/Create Case

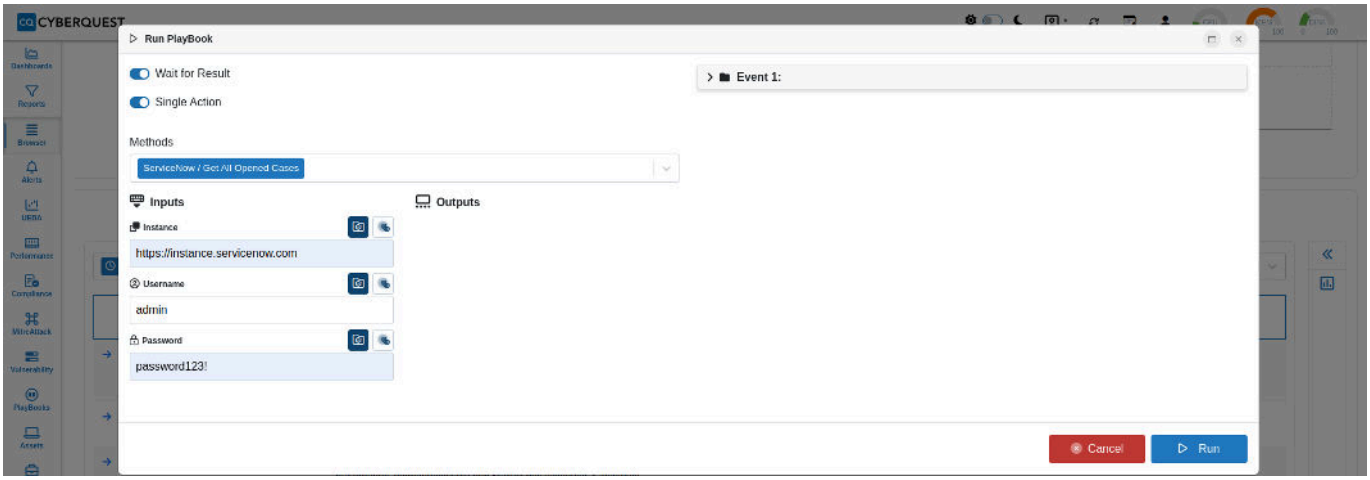
Create a case (it is used in pricipal for external entities).


Run PlayBook
Wait for Result
Single Action
Methods
ServiceNow / Create Case
Inputs
Outputs
Event 1:
Instance
https://instance.servicenow.com
Username
admin
Password
password123!
Consumer
Contact Type
Priority
Short description
Description
Urgency
Impact
Assignment Group
Assigned To
cmdb_ci
Category
State
Location
Business Service
Due Date
Cancel
Run

Inputs	Description
Instance (is required)	The subdomain created using ServiceNow, for example: nextgensoftware
Username (is required)	To use this API you must have an account valid account on ServiceNow. Use the username used to login in ServiNow Interface
Password (is required)	To use this API you must have an account valid account on ServiceNow. Use the password used to login in ServiNow Interface
Consumer	The type of the consumer
Contact Type	Describes how the incident was reported (e.g., phone, email). Helps in tracking and analyzing reporting methods.
Priority	Usually calculated automatically from urgency and impact, but can be set manually if needed. It determines the order in which incidents are addressed
Short description	A brief summary of the issue. This is a required field to give a quick overview of the incident.
Description	A detailed description of the case. This field provides essential context and details about the problem.
Urgency	Indicates how quickly the case needs to be addressed. This affects the priority of the case.
Impact	Describes the impact level of the case on the business. This, along with urgency, helps to determine the cases priority.
Assignment Group	The group responsible for resolving the case. Ensures the case is routed to the correct team.
Assigned To	The specific individual assigned to handle the case. This is crucial for accountability and tracking progress.
cmdb_ci	Links the incident to a specific Configuration Item (CI) in the CMDB. Helps in identifying which asset or service is affected.
Category	Specifies the type of issue (e.g., software, hardware). Helps in categorizing and routing the case appropriately.
State	Indicates the current status of the incident (e.g., New, In Progress). Useful for tracking the cases lifecycle.
Location	Indicates the current status of the incident (e.g., New, In Progress). Useful for tracking the cases lifecycle.
Business Service	Links the incident to a specific business service. This is crucial for understanding the impact on business operations.
Due Date	The deadline for resolving the case. Helps in managing and meeting SLAs.

ServiceNow/Get All Opened Cases

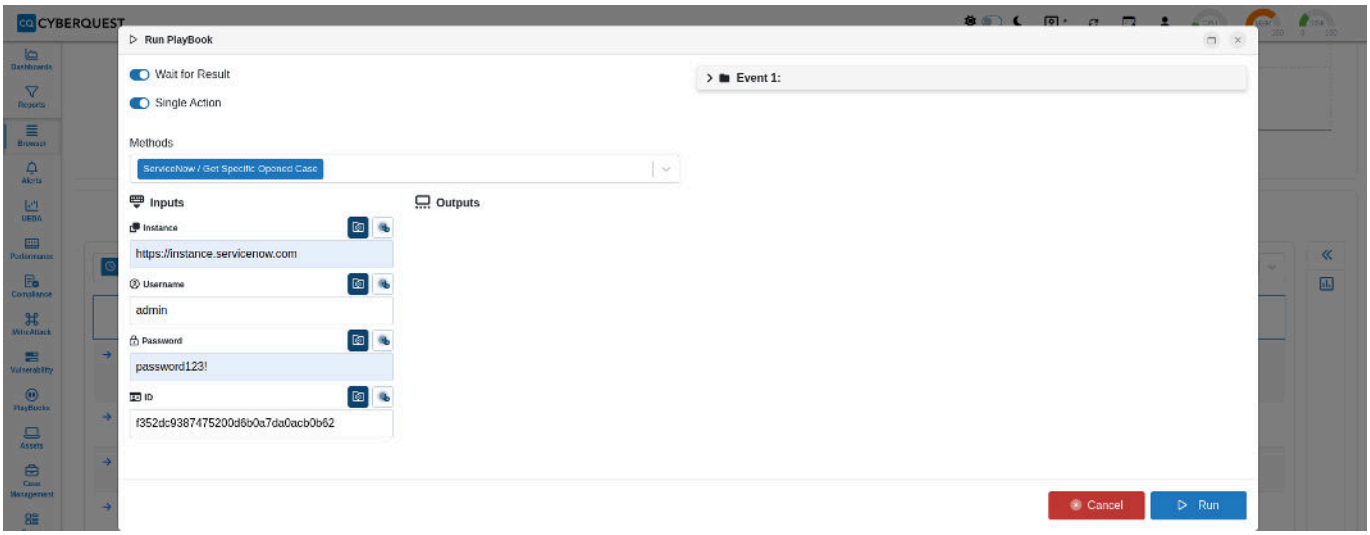
Get all opened cases.



Inputs	Description
Instance (is required)	The subdomain created using ServiceNow, for example: nextgensoftware
Username (is required)	To use this API you must have an account valid account on ServiceNow. Use the username used to login in ServiNow Interface
Password (is required)	To use this API you must have an account valid account on ServiceNow. Use the password used to login in ServiNow Interface

ServiceNow/Get Specific Opened Case

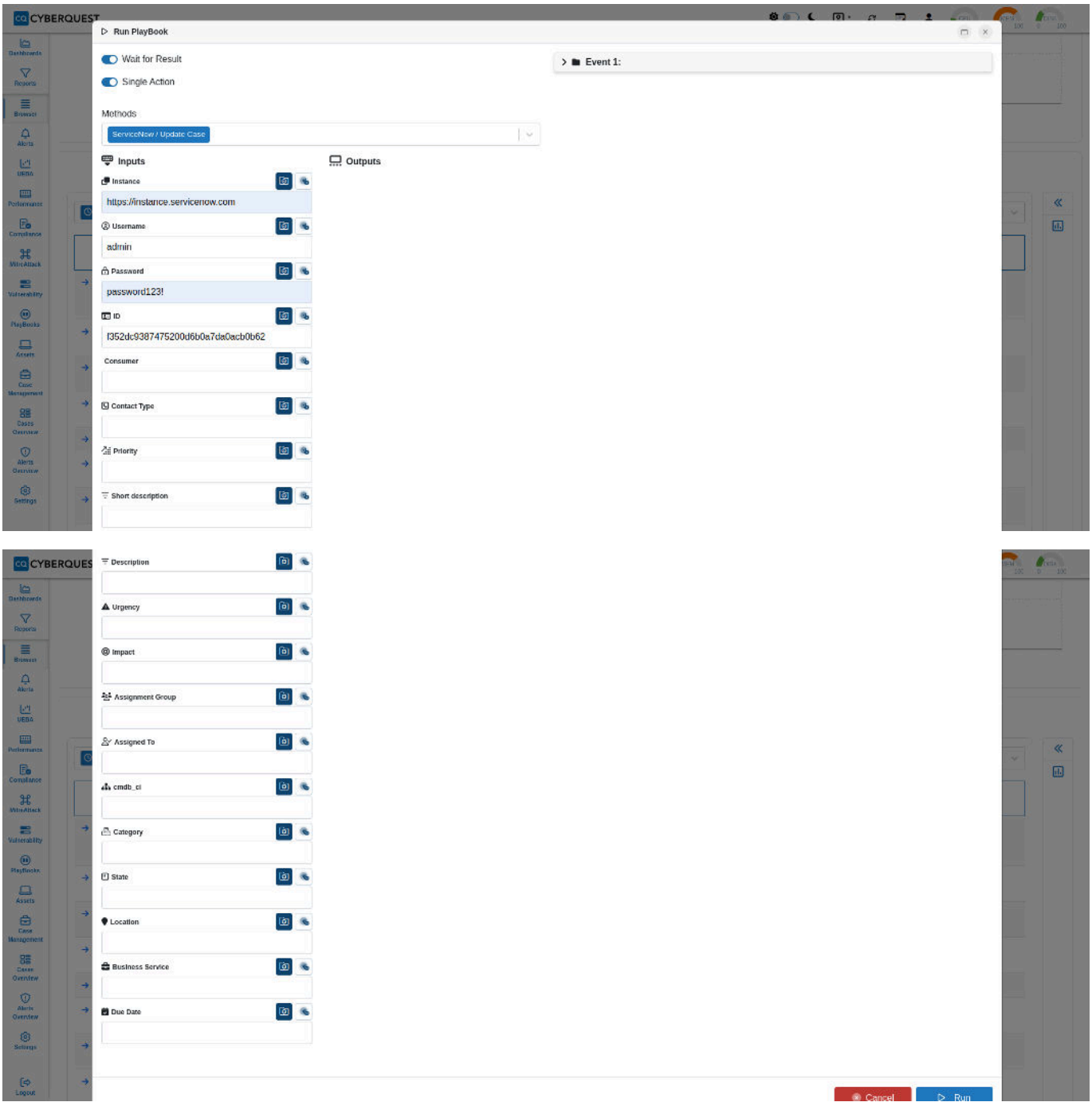
Get all opened cases.



Inputs	Description
Instance (is required)	The subdomain created using ServiceNow, for example: nextgensoftware
Username (is required)	To use this API you must have an account valid account on ServiceNow. Use the username used to login in ServiNow Interface
Password (is required)	To use this API you must have an account valid account on ServiceNow. Use the password used to login in ServiNow Interface
ID (is required)	The ID of the Opened Case you want to retrieve

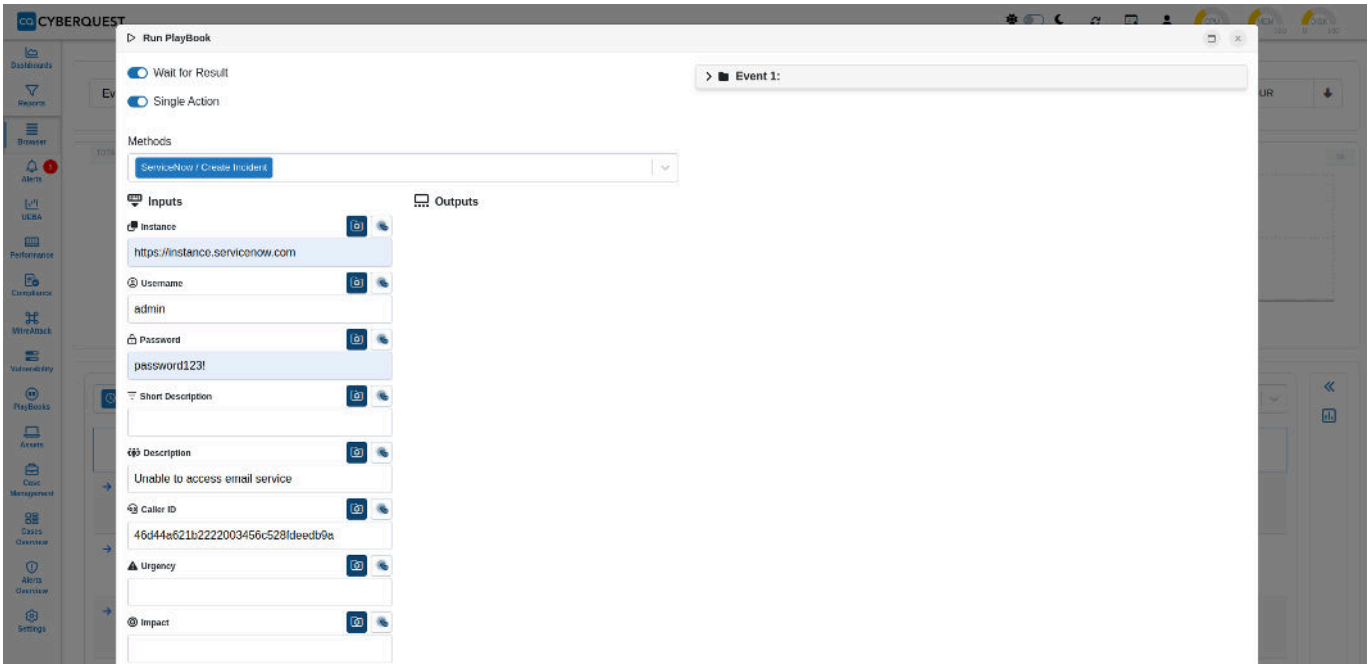
ServiceNow/Update Case

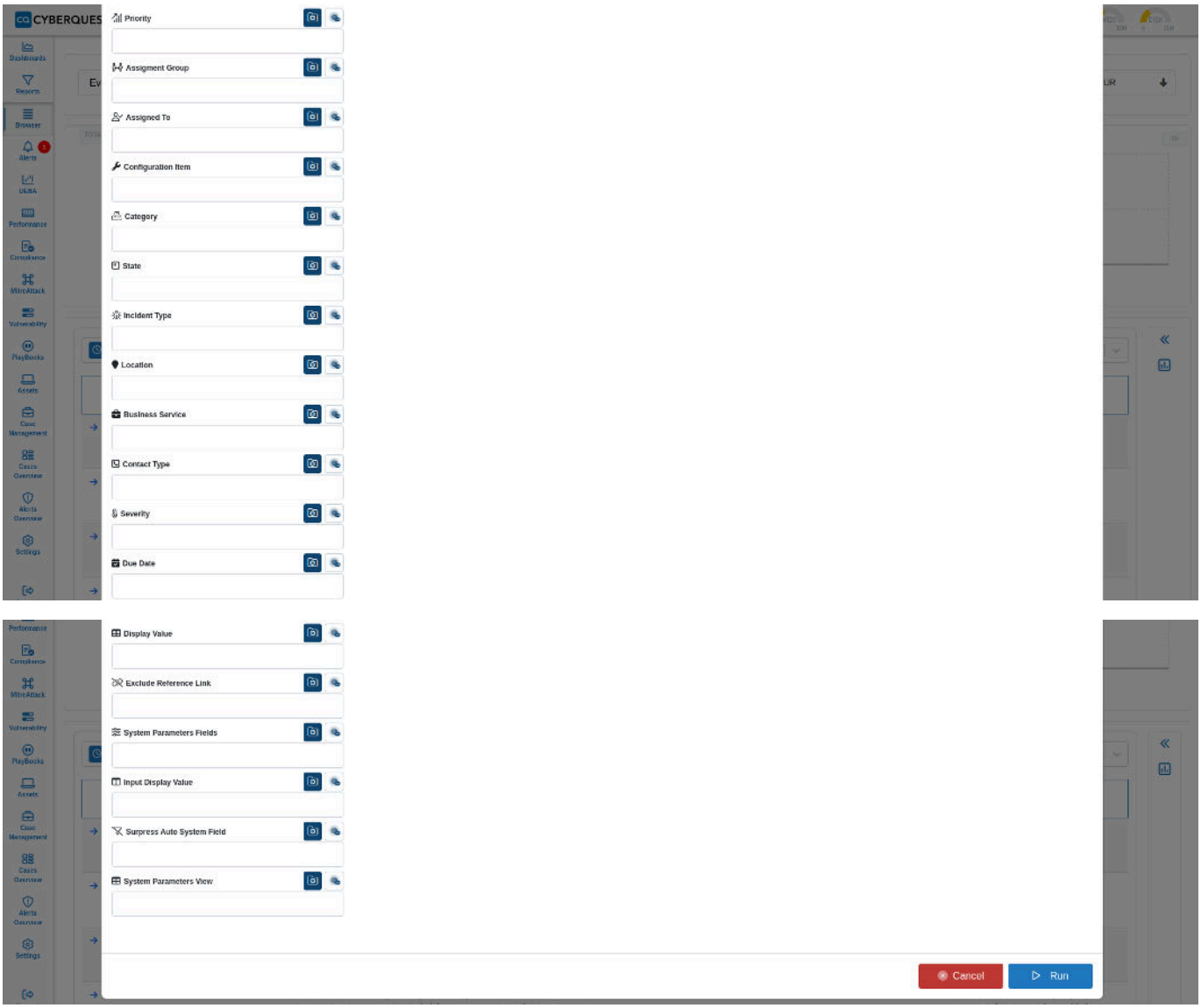
Update an opened case.


CYBERQUEST
Run PlayBook
Wait for Result
Single Action
Methods
ServiceNow / Update Case
Inputs
Outputs
Event 1:
Instance
https://instance.servicenow.com
Username
admin
Password
password123!
ID
f352dc9387475200d6b0a7da0acb0b62
Consumer
Contact Type
Priority
Short description
Description
Urgency
Impact
Assignment Group
Assigned To
cmdb_ci
Category
State
Location
Business Service
Due Date
Cancel
Run

Inputs	Description
Instance (is required)	The subdomain created using ServiceNow, for example: nextgensoftware
Username (is required)	To use this API you must have an account valid account on ServiceNow. Use the username used to login in ServiNow Interface
Password (is required)	To use this API you must have an account valid account on ServiceNow. Use the password used to login in ServiNow Interface
Consumer	The type of the consumer
Contact Type	Describes how the incident was reported (e.g., phone, email). Helps in tracking and analyzing reporting methods.
Priority	Usually calculated automatically from urgency and impact, but can be set manually if needed. It determines the order in which incidents are addressed
Short description	A brief summary of the issue. This is a required field to give a quick overview of the incident.
Description	A detailed description of the case. This field provides essential context and details about the problem.
Urgency	Indicates how quickly the case needs to be addressed. This affects the priority of the case.
Impact	Describes the impact level of the case on the business. This, along with urgency, helps to determine the cases priority.
Assignment Group	The group responsible for resolving the case. Ensures the case is routed to the correct team.
Assigned To	The specific individual assigned to handle the case. This is crucial for accountability and tracking progress.
cmdb_ci	Links the incident to a specific Configuration Item (CI) in the CMDB. Helps in identifying which asset or service is affected.
Category	Specifies the type of issue (e.g., software, hardware). Helps in categorizing and routing the case appropriately.
State	Indicates the current status of the incident (e.g., New, In Progress). Useful for tracking the cases lifecycle.
Location	Indicates the current status of the incident (e.g., New, In Progress). Useful for tracking the cases lifecycle.
Business Service	Links the incident to a specific business service. This is crucial for understanding the impact on business operations.
Due Date	The deadline for resolving the case. Helps in managing and meeting SLAs.

ServiceNow/Create Incident

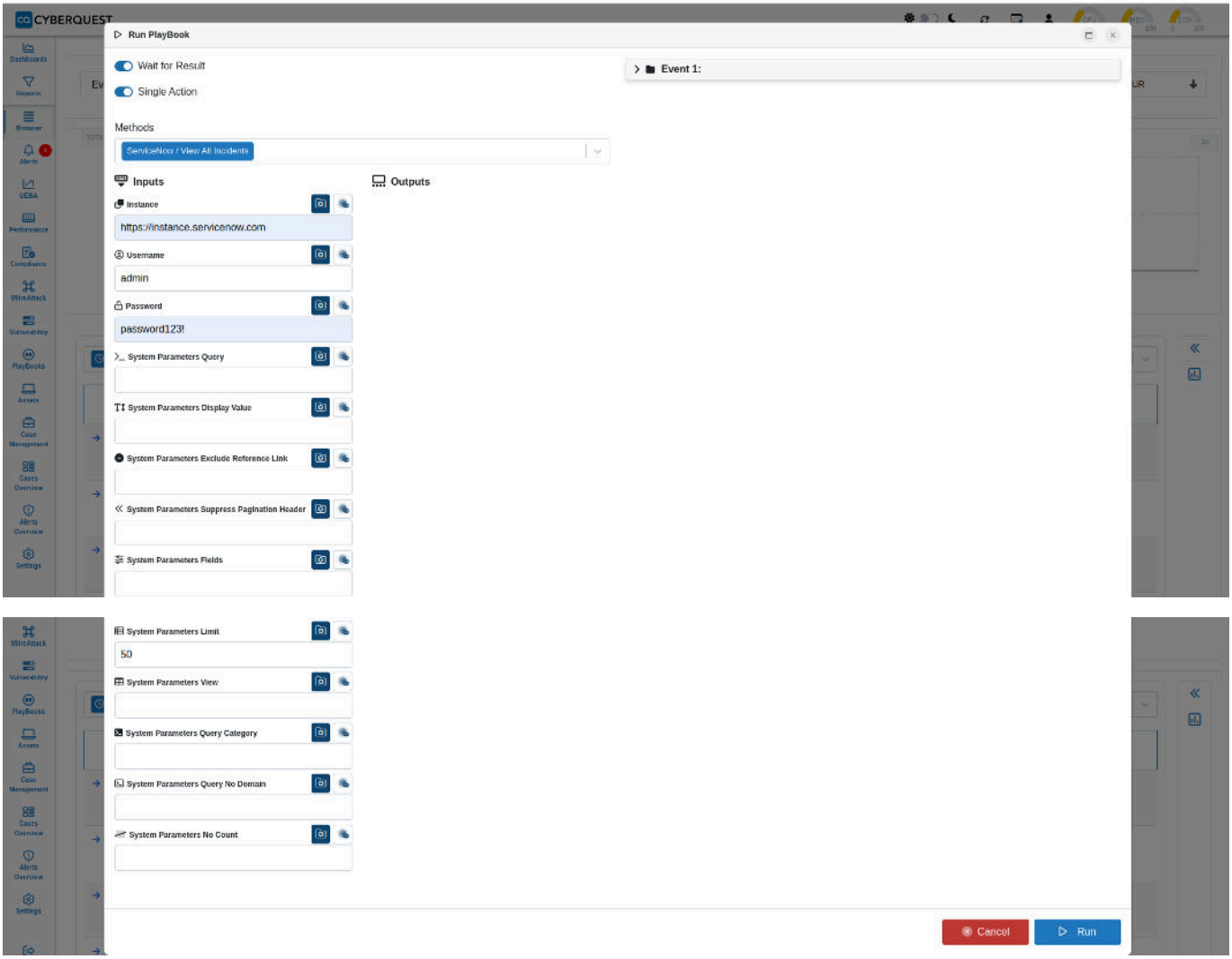



Priority
Assigment Group
Assigned To
Configuration Item
Category
State
Incident Type
Location
Business Service
Contact Type
Severity
Due Date
Display Value
Exclude Reference Link
System Parameters Fields
Input Display Value
Surpress Auto System Field
System Parameters View
Cancel
Run

Inputs	Description
Instance (is required)	The subdomain created using ServiceNow, for example: nextgensoftware
Username (is required)	To use this API you must have an account valid account on ServiceNow. Use the username used to login in ServiNow Interface
Password (is required)	To use this API you must have an account valid account on ServiceNow. Use the password used to login in ServiNow Interface
Short description	A brief summary of the issue. This is a required field to give a quick overview of the incident.
Description	A detailed description of the case. This field provides essential context and details about the problem.
Caller ID	Specifies the user or person who reported the incident. This is important for tracking and follow-up.
Urgency	Indicates how quickly the case needs to be addressed. This affects the priority of the case.
Impact	Describes the impact level of the case on the business. This, along with urgency, helps to determine the cases priority.
Priority	Usually calculated automatically from urgency and impact, but can be set manually if needed. It determines the order in which incidents are addressed
Assignment Group	The group responsible for resolving the case. Ensures the case is routed to the correct team.
Assigned To	The specific individual assigned to handle the case. This is crucial for accountability and tracking progress.
cmdb_ci	Links the incident to a specific Configuration Item (CI) in the CMDB. Helps in identifying which asset or service is affected.
Category	Specifies the type of issue (e.g., software, hardware). Helps in categorizing and routing the case appropriately.
State	Indicates the current status of the incident (e.g., New, In Progress). Useful for tracking the cases lifecycle.
Incident Type	Defines the nature of the incident (e.g., inquiry, failure). Helps in understanding and prioritizing the incident.
Location	Indicates the current status of the incident (e.g., New, In Progress). Useful for tracking the cases lifecycle.
Business Service	Links the incident to a specific business service. This is crucial for understanding the impact on business operations.
Contact Type	Describes how the incident was reported (e.g., phone, email). Helps in tracking and analyzing reporting methods.
Severity	Describes how the incident was reported (e.g., phone, email). Helps in tracking and analyzing reporting methods.
Due Date	The deadline for resolving the case. Helps in managing and meeting SLAs.
Display Value	Return field display values (true), actual values (false), or both (all) (default: false
Exclude Reference Link	True to exclude Table API links for reference fields (default: false)
System Parameters Fields	A comma-separated list of fields to return in the response
Input Display Value	Set field values using their display value (true) or actual value (false) (default: false)
Surpress Auto System Field	True to suppress auto generation of system fields (default: false)
System Parameters View	Render the response according to the specified UI view (overridden by System Parameters Fields)

ServiceNow/View All Incidents

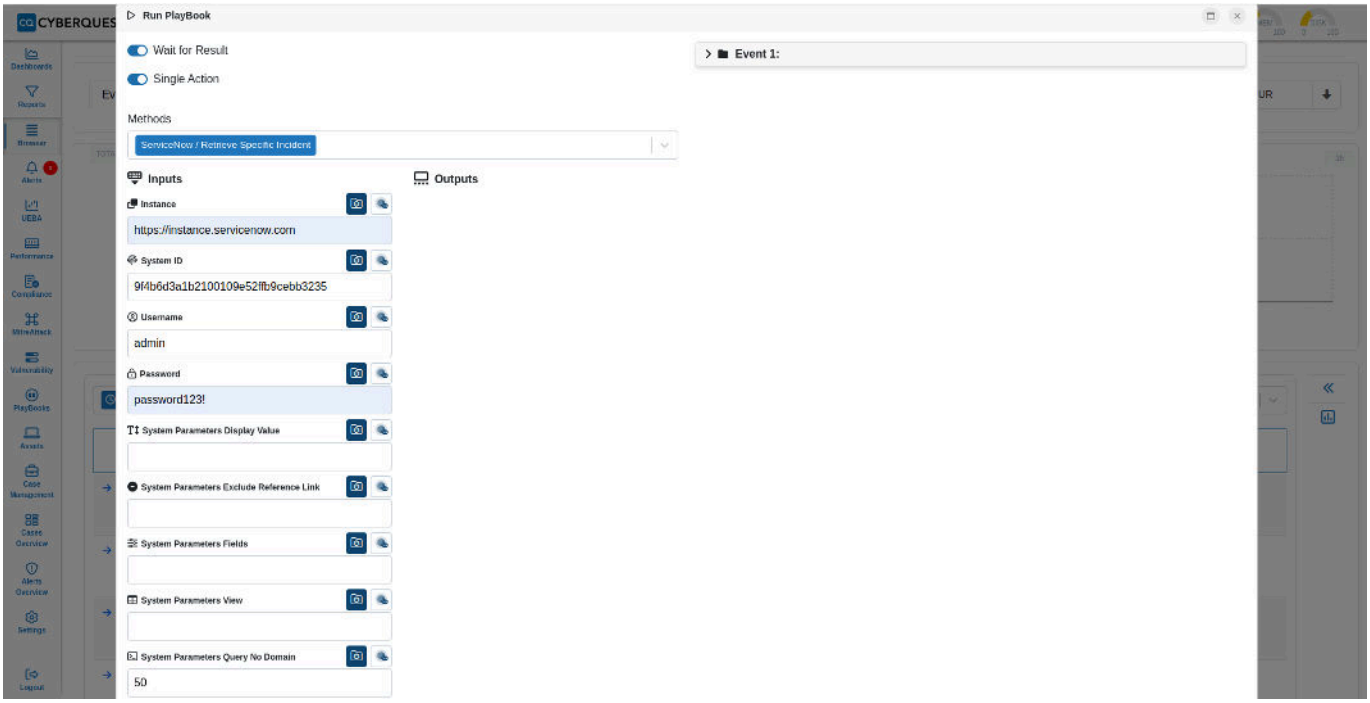
View all incidents created.



Inputs	Description
Instance (is required)	The subdomain created using ServiceNow, for example: nextgensoftware
Username (is required)	To use this API you must have an account valid account on ServiceNow. Use the username used to login in ServiNow Interface
Password (is required)	To use this API you must have an account valid account on ServiceNow. Use the password used to login in ServiNow Interface
System Parameters Query	An encoded query string used to filter the results
System Parameters Display Value	Return field display values (true), actual values (false), or both (all) (default: false)
System Parameters Exclude Reference Link	True to exclude Table API links for reference fields (default: false)
System Parameters Suppress Pagination Header	True to supress pagination header (default: false)
System Parameters Fields	A comma-separated list of fields to return in the response
System Parameters Limit	The maximum number of results returned per page (default: 10,000)
System Parameters View	Render the response according to the specified UI view (overridden by sysparm_fields)
System Parameters Query Category	Name of the query category (read replica category) to use for queries
System Parameters Query No Domain	True to access data across domains if authorized (default: false)
System Parameters No Count	Do not execute a select count(*) on table (default: false)

ServiceNow/Retrieve Specific Incident

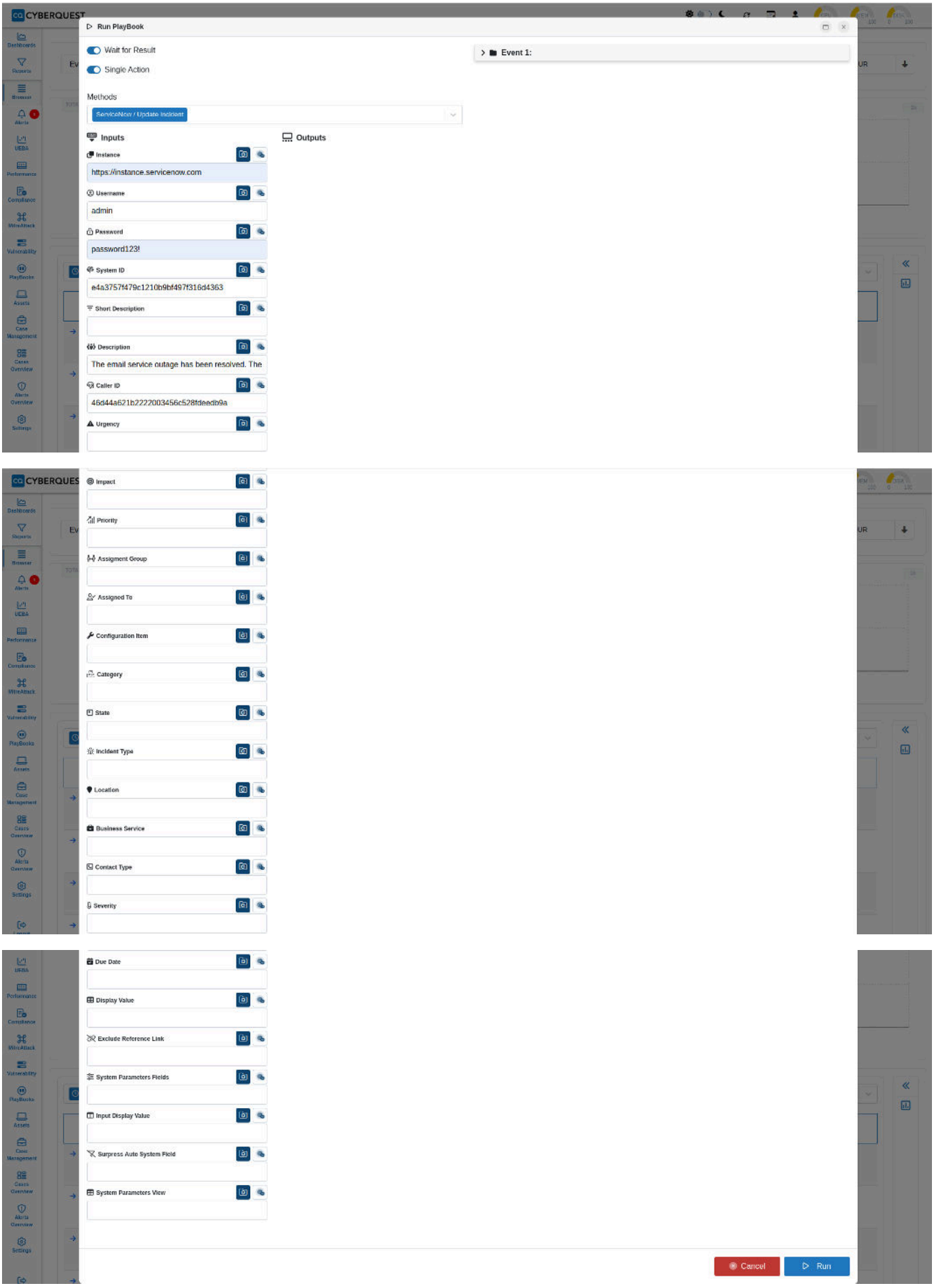
View specific incident.



Inputs	Description
Instance (is required)	The subdomain created using ServiceNow, for example: nextgensoftware
System ID (is required)	The ID generated from the system when the incident was created
Username (is required)	To use this API you must have an account valid account on ServiceNow. Use the username used to login in ServiNow Interface
Password (is required)	To use this API you must have an account valid account on ServiceNow. Use the password used to login in ServiNow Interface
System Parameters Display Value	Return field display values (true), actual values (false), or both (all) (default: false)
System Parameters Exclude Reference Link	True to exclude Table API links for reference fields (default: false)
System Parameters Fields	A comma-separated list of fields to return in the response
System Parameters View	Render the response according to the specified UI view (overridden by sysparm_fields)
System Parameters Query No Domain	True to access data across domains if authorized (default: false)

ServiceNow/Update Incident

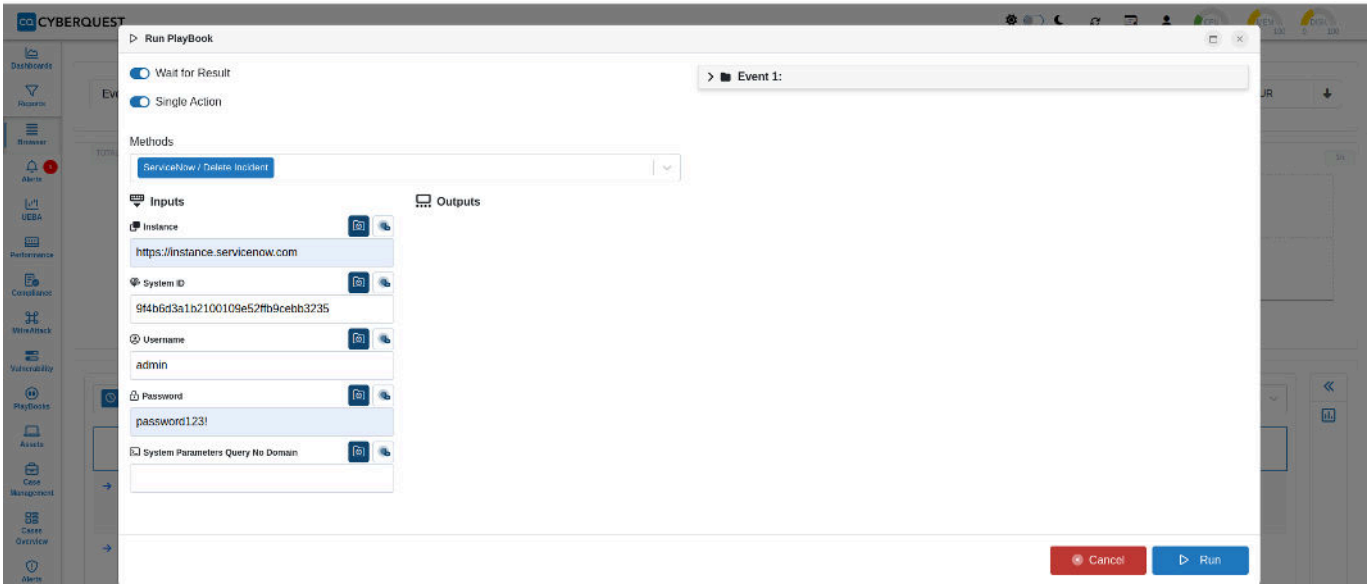
Update incident parameters.


CYBERQUEST
Run PlayBook
Wait for Result
Single Action
Event 1:
Methods
ServiceNow / Update Incident
Inputs
Outputs
Instance
https://instance.servicenow.com
Username
admin
Password
password123!
System ID
e4a3757f479c1210b9bf497f316d4363
Short Description
Description
The email service outage has been resolved. The
Caller ID
46d44a621b2222003456c528fdeedb9a
Urgency
Impact
Priority
Assigment Group
Assigned To
Configuration Item
Category
State
Incident Type
Location
Business Service
Contact Type
Severity
Due Date
Display Value
Exclude Reference Link
System Parameters Fields
Input Display Value
Surpress Auto System Field
System Parameters View
Cancel
Run

Inputs	Description
Instance (is required)	The subdomain created using ServiceNow, for example: nextgensoftware
Username (is required)	To use this API you must have an account valid account on ServiceNow. Use the username used to login in ServiNow Interface
System ID (is required)	The ID generated from the system when the incident was created
Short description	A brief summary of the issue. This is a required field to give a quick overview of the incident.
Description	A detailed description of the case. This field provides essential context and details about the problem.
Caller ID	Specifies the user or person who reported the incident. This is important for tracking and follow-up.
Urgency	Indicates how quickly the case needs to be addressed. This affects the priority of the case.
Impact	Describes the impact level of the case on the business. This, along with urgency, helps to determine the cases priority.
Priority	Usually calculated automatically from urgency and impact, but can be set manually if needed. It determines the order in which incidents are addressed
Assignment Group	The group responsible for resolving the case. Ensures the case is routed to the correct team.
Assigned To	The specific individual assigned to handle the case. This is crucial for accountability and tracking progress.
Configuration Item	Links the incident to a specific Configuration Item (CI) in the CMDB. Helps in identifying which asset or service is affected.
Category	Specifies the type of issue (e.g., software, hardware). Helps in categorizing and routing the case appropriately.
State	Indicates the current status of the incident (e.g., New, In Progress). Useful for tracking the cases lifecycle.
Incident Type	Defines the nature of the incident (e.g., inquiry, failure). Helps in understanding and prioritizing the incident.
Location	Indicates the current status of the incident (e.g., New, In Progress). Useful for tracking the cases lifecycle.
Business Service	Links the incident to a specific business service. This is crucial for understanding the impact on business operations.
Contact Type	Describes how the incident was reported (e.g., phone, email). Helps in tracking and analyzing reporting methods.
Severity	Describes how the incident was reported (e.g., phone, email). Helps in tracking and analyzing reporting methods.
Due Date	The deadline for resolving the case. Helps in managing and meeting SLAs.
Display Value	Return field display values (true), actual values (false), or both (all) (default: false
Exclude Reference Link	True to exclude Table API links for reference fields (default: false)
System Parameters Fields	A comma-separated list of fields to return in the response
Input Display Value	Set field values using their display value (true) or actual value (false) (default: false)
Surpress Auto System Field	True to suppress auto generation of system fields (default: false)
System Parameters View	Render the response according to the specified UI view (overridden by System Parameters Fields)

ServiceNow/Delete Incident

Delete an incident.

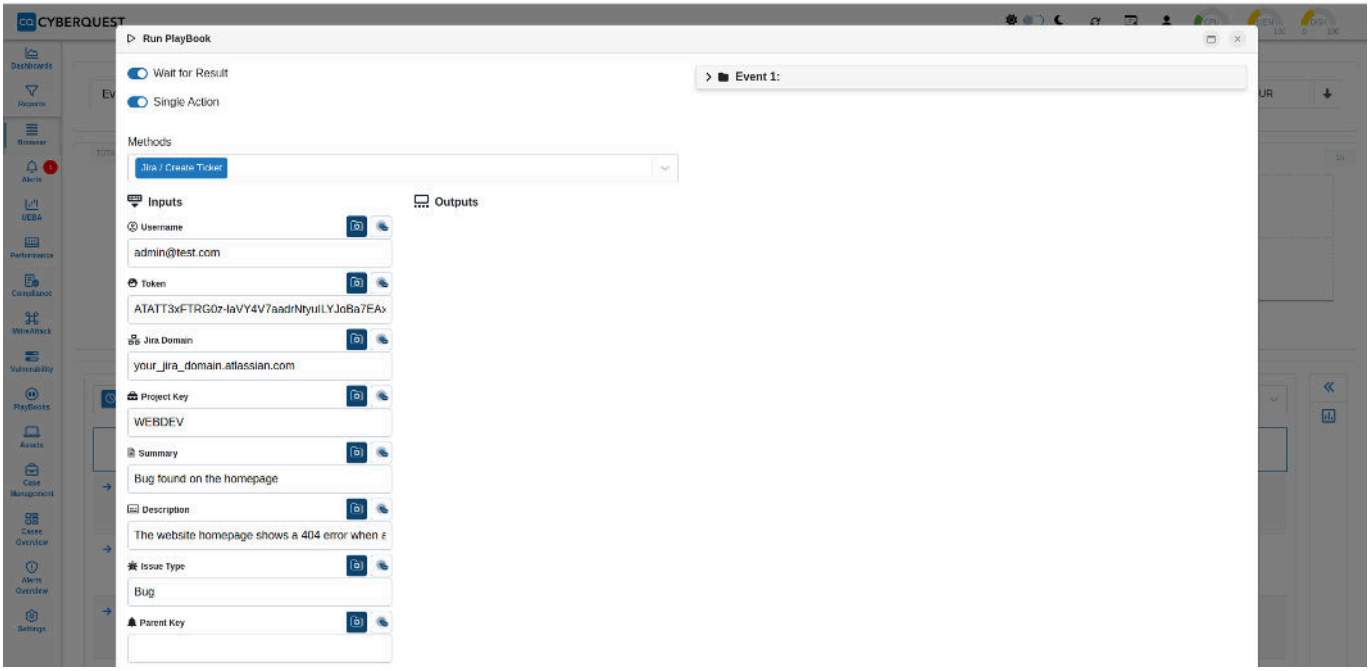


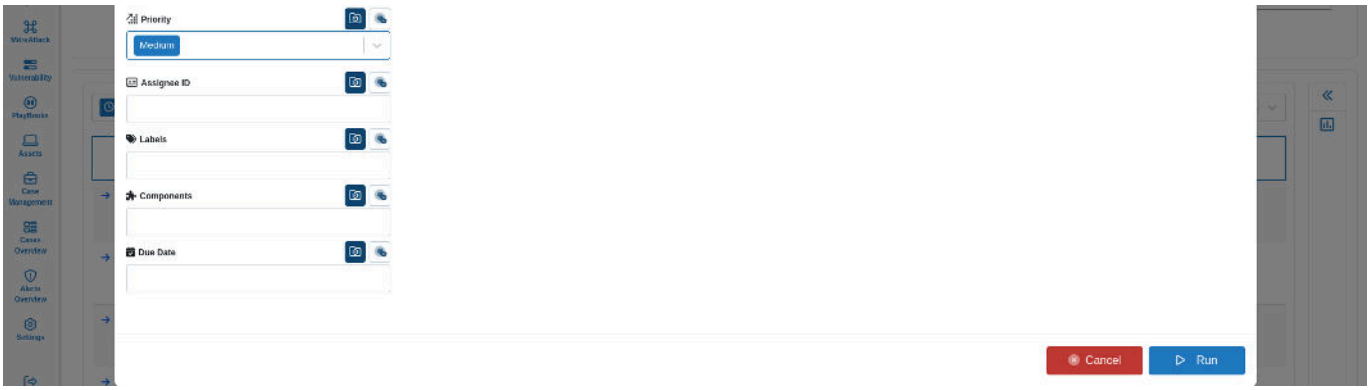
Inputs	Description
Instance (is required)	The subdomain created using ServiceNow, for example: nextgensoftware
System ID (is required)	The ID generated from the system when the incident was created
Username (is required)	To use this API you must have an account valid account on ServiceNow. Use the username used to login in ServiNow Interface
Password (is required)	To use this API you must have an account valid account on ServiceNow. Use the password used to login in ServiNow Interface
System Parameters Query No Domain	True to access data across domains if authorized (default: false)

Jira

Jira/Create Ticket

Create a JIRA Ticket.

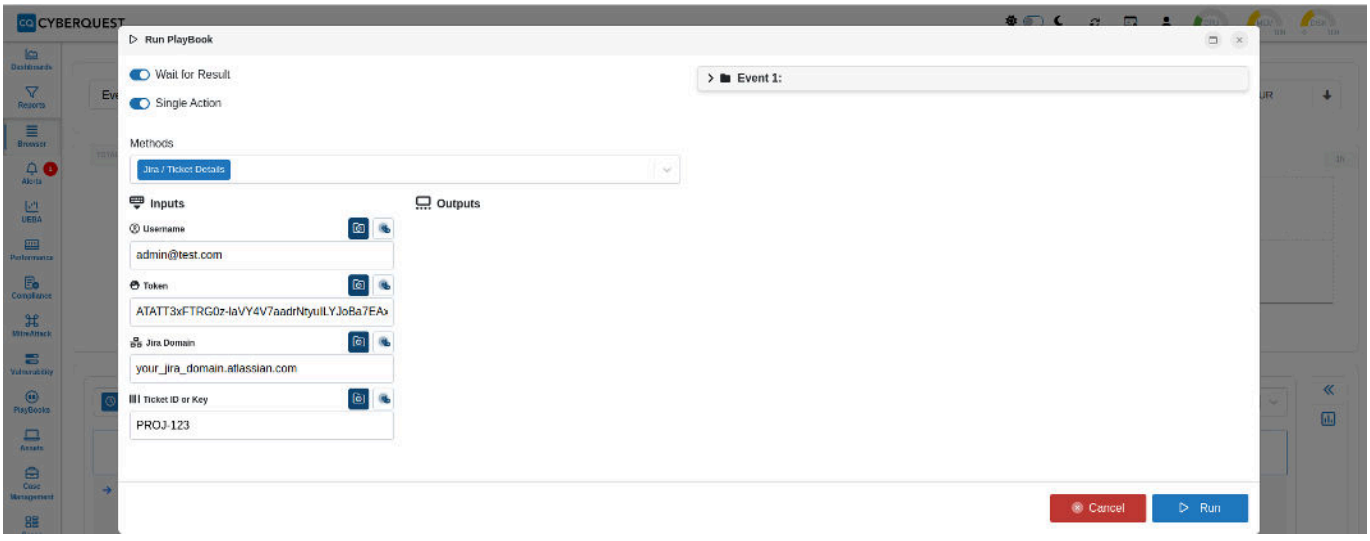




Inputs	Description
Username (is required)	Your account has a username set up to access the Jira server
Token(is required)	Your account has an API token to access the Jira server
Jira Domain (is required)	Your Jira domain(ex: your_jira_domain.atlassian.com)
Project Key (is required)	“Specify the project ID that corresponds to the project where you want to create the Jira ticket.
Summary (is required)	Title for the new Jira ticket.
Description (is required)	Write a description for the new Jira ticket.
Issue Type (is required)	Specify the type of ticket to create
Parent Key	When creating a subtask, you must provide the ID of the parent ticket. This field is only relevant for subtask ticket types. For instance, Test-1.
Priority (is required)	Choose a priority for the Jira ticket update: Highest, High, Medium, Low, or Lowest.
Assignee ID	The person you want to assign the ticket
Labels	Keywords or tags used to categorize and organize Jira tickets.
Components	Specifies the components associated with a Jira ticket
Due Date	Time until the ticket must be resolved

Jira/Ticket Details

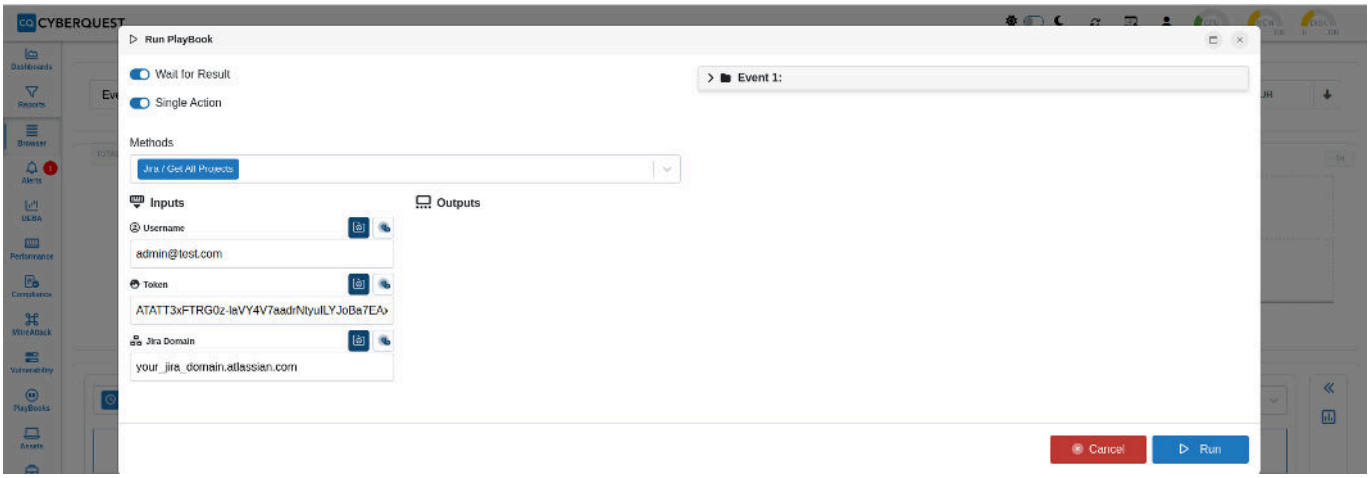
Return details for a ticket.



Inputs	Description
Username (is required)	Your account has a username set up to access the Jira server
Token(is required)	Your account has an API token to access the Jira server
Jira Domain (is required)	Your Jira domain(ex: your_jira_domain.atlassian.com)
Ticket ID or Key (is required)	The ID or key of the issue.he ID or key of the issue.

Jira/Get All Projects

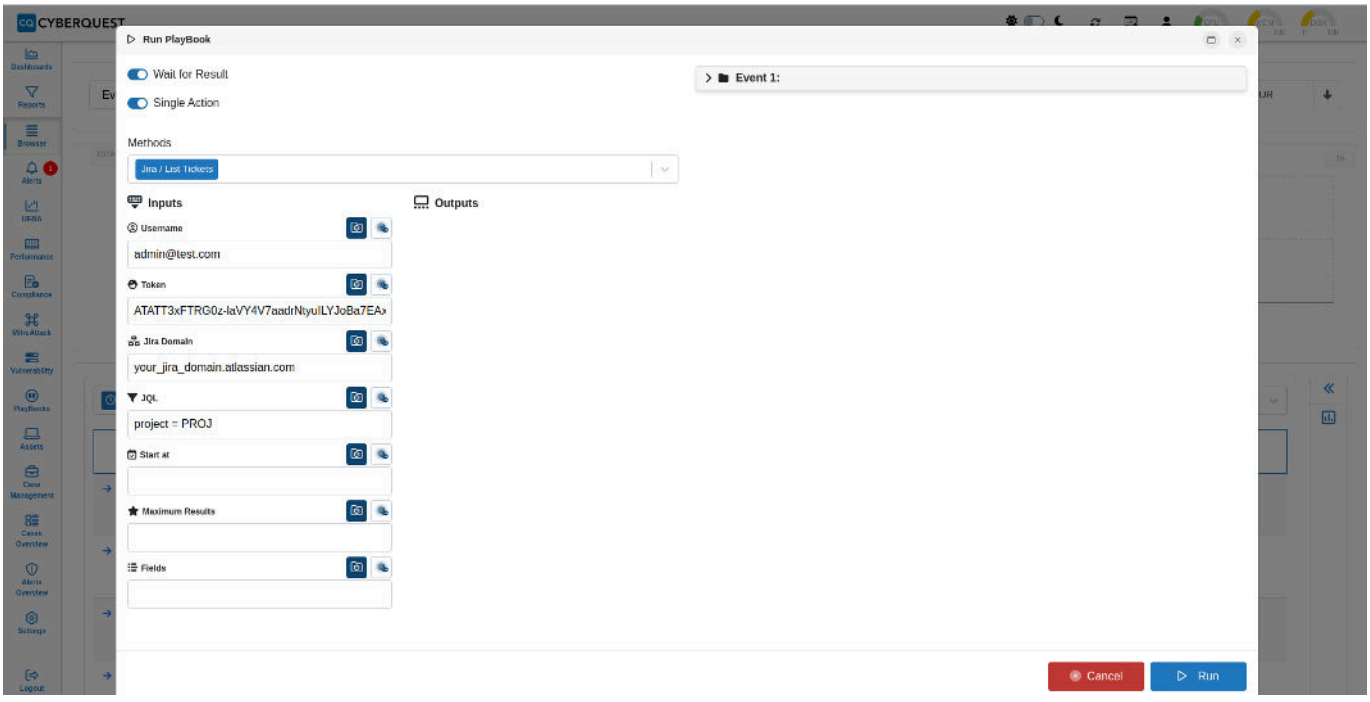
Return all projects.



Inputs	Description
Username (is required)	Your account has a username set up to access the Jira server
Token(is required)	Your account has an API token to access the Jira server
Jira Domain (is required)	Your Jira domain(ex: your_jira_domain.atlassian.com)

Jira/List Tickets

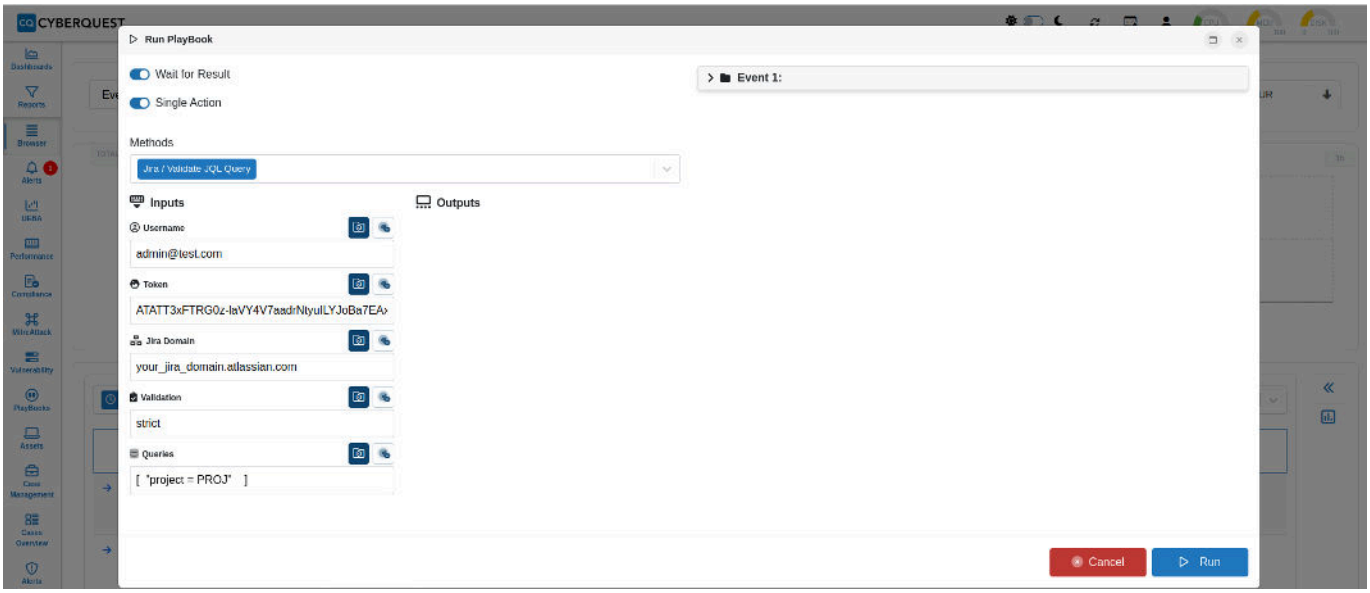
Searches for issues using JQL.



Inputs	Description
Username (is required)	Your account has a username set up to access the Jira server
Token(is required)	Your account has an API token to access the Jira server
Jira Domain (is required)	Your Jira domain(ex: your_jira_domain.atlassian.com)
JQL (is required)	Construct a Jira query to identify and list tickets that meet specific criteria. You must define at least one search filter, for instance, project = project_id
Start at	The index of the first item to return in the page of results (page offset). The base index is 0
Maximum Results	The maximum number of items to return per page. Default: 50
Fields	A list of fields to return for each issue, use it to retrieve a subset of fields. This parameter accepts a comma-separated list. Expand options include: - all Returns all fields. - *navigable Returns navigable fields. - Any issue field, prefixed with a minus to exclude. - The default is *navigable

Jira/Validate JQL Query

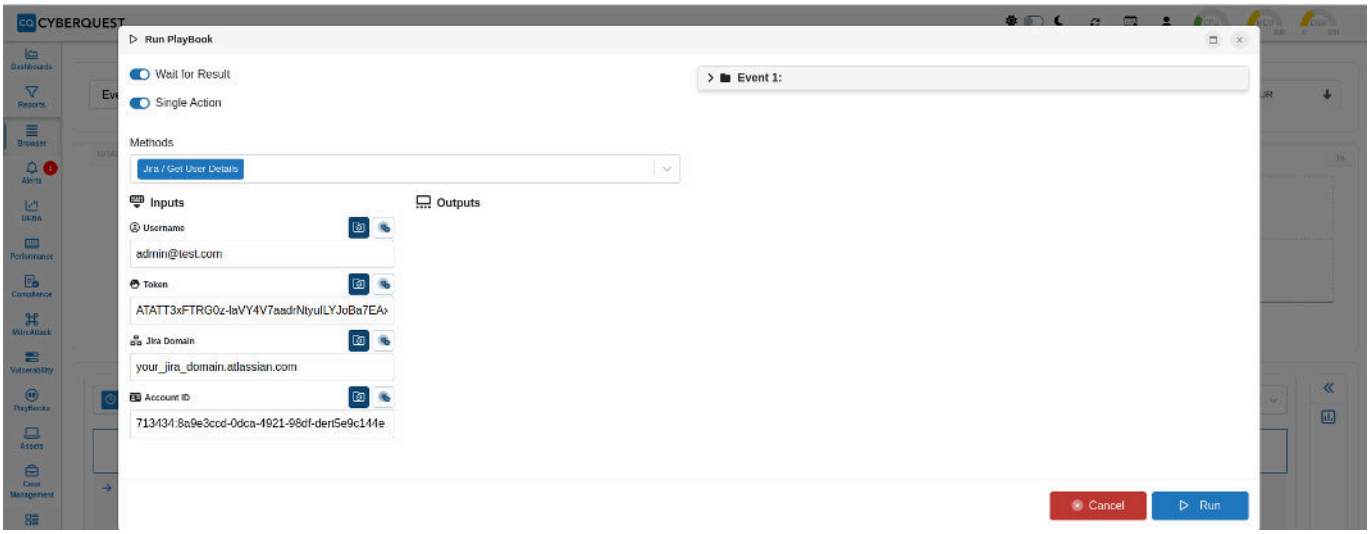
Parses and validates JQL queries.



Inputs	Description
Username (is required)	Your account has a username set up to access the Jira server
Token (is required)	Your account has an API token to access the Jira server
Jira Domain (is required)	Your Jira domain(ex: your_jira_domain.atlassian.com)
Validation (is required)	How to validate the JQL query and treat the validation results. Validation options include: - strict Returns all errors. If validation fails, the query structure is not returned. - warn Returns all errors. If validation fails but the JQL query is correctly formed, the query structure is returned. - none No validation is performed. If JQL query is correctly formed, the query structure is returned. - Default: strict - Valid values: strict, warn, none
Queries (is required)	A list of queries to parse. Min length: 1

Jira/Get User Details

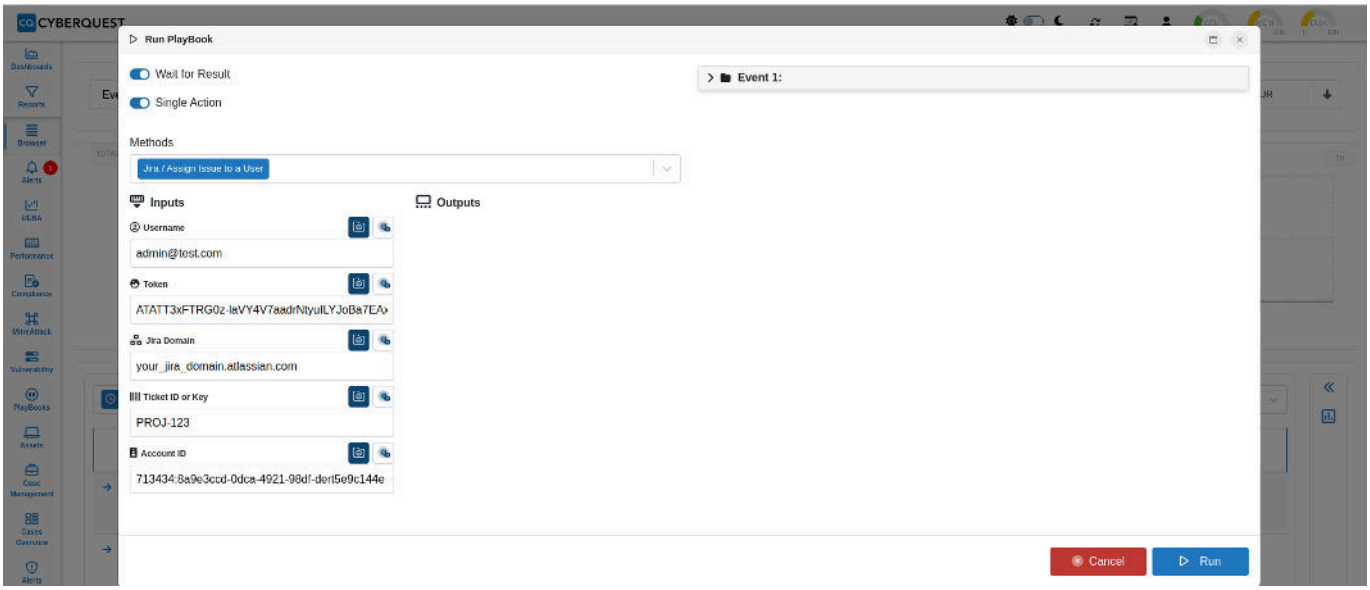
Return details for a user.



Inputs	Description
Username (is required)	Your account has a username set up to access the Jira server
Token(is required)	Your account has an API token to access the Jira server
Jira Domain (is required)	Your Jira domain(ex: your_jira_domain.atlassian.com)
Account ID (is required)	The account ID of the user, which uniquely identifies the user across all Atlassian products. For example, 5b10ac8d82e05b22cc7d4ef5.

Jira/Assign Issue to a User

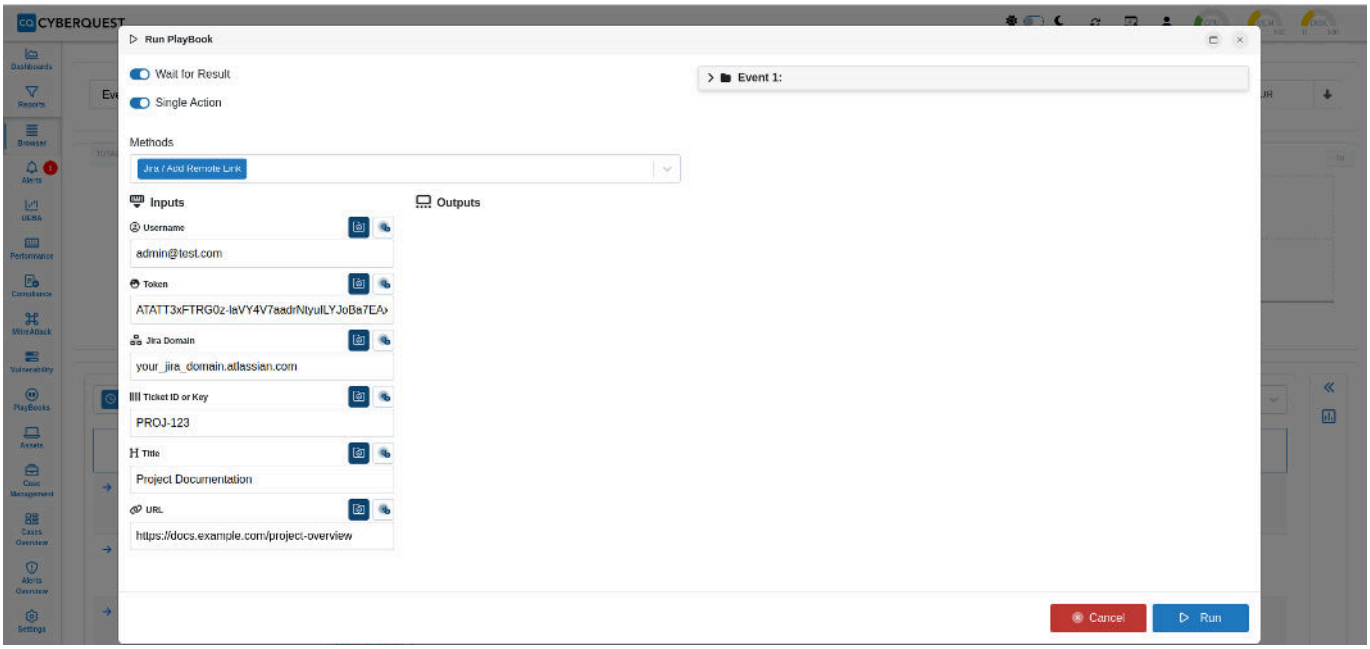
Assigns an issue to a user.



Inputs	Description
Username (is required)	Your account has a username set up to access the Jira server
Token(is required)	Your account has an API token to access the Jira server
Jira Domain (is required)	Your Jira domain(ex: your_jira_domain.atlassian.com)
Ticket ID or Key (is required)	The ID or key of the issue.
Account ID (is required)	The account ID of the user, which uniquely identifies the user across all Atlassian products. For example, 5b10ac8d82e05b22cc7d4ef5.

Jira/Add Remote Link

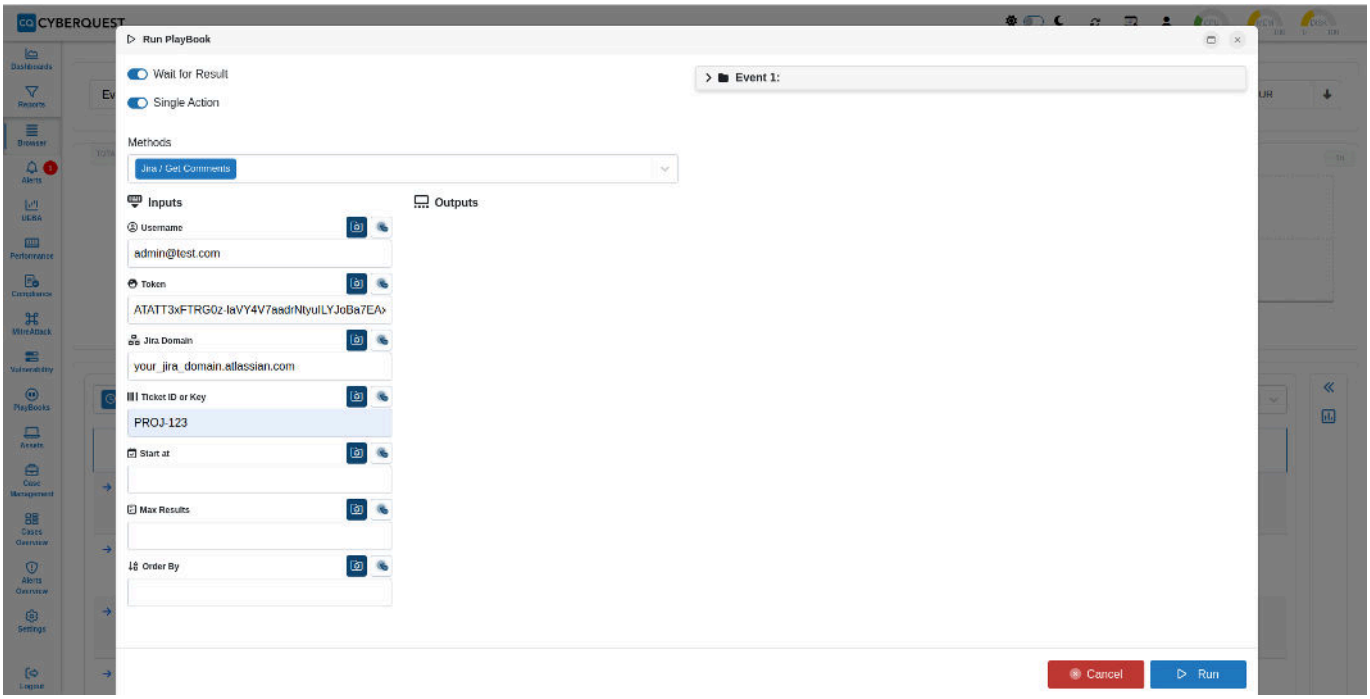
Creates or updates a remote issue link for an issue.



Inputs	Description
Username (is required)	Your account has a username set up to access the Jira server
Token(is required)	Your account has an API token to access the Jira server
Jira Domain (is required)	Your Jira domain(ex: your_jira_domain.atlassian.com)
Ticket ID or Key (is required)	The ID or key of the issue.
Title (is required)	The title of the item.
URL (is required)	The URL of the item.

Jira/Get Comments

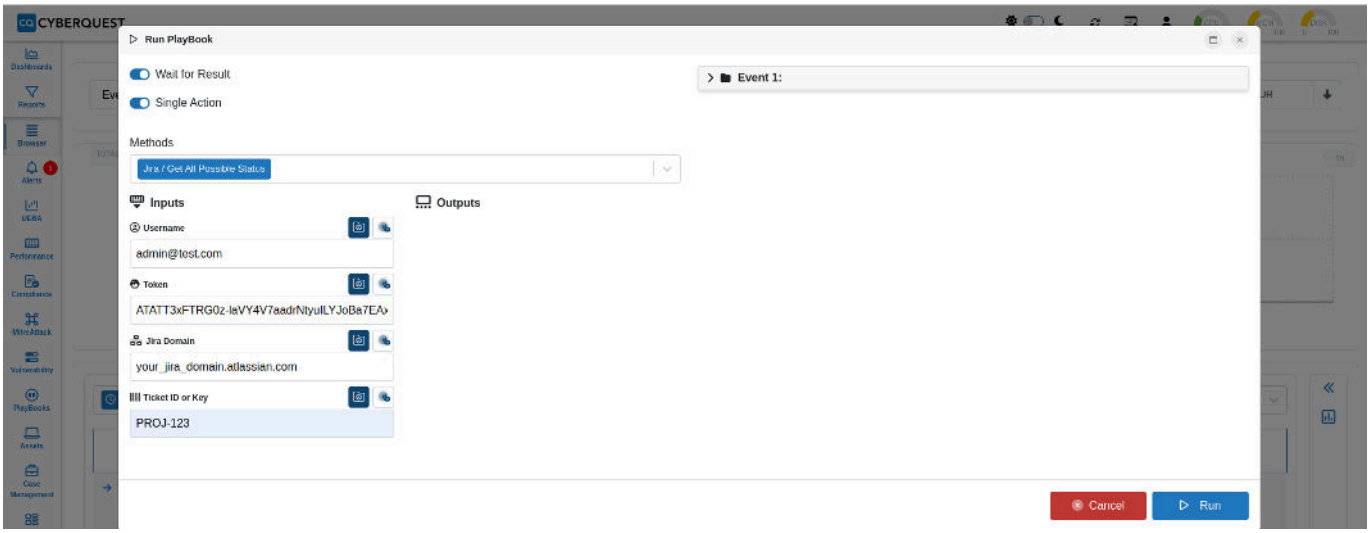
Returns all comments for an issue.



Inputs	Description
Username (is required)	Your account has a username set up to access the Jira server
Token(is required)	Your account has an API token to access the Jira server
Jira Domain (is required)	Your Jira domain(ex: your_jira_domain.atlassian.com)
Ticket ID or Key (is required)	The ID or key of the issue.
Start at	The index of the first item to return in a page of results (page offset).Default: 0
Max Results	The maximum number of items to return per page. Default: 5000
Order By	Order the results by a field. Accepts created to sort comments by their created date. Valid values: created, -created, +created

Jira/Get All Possible Status

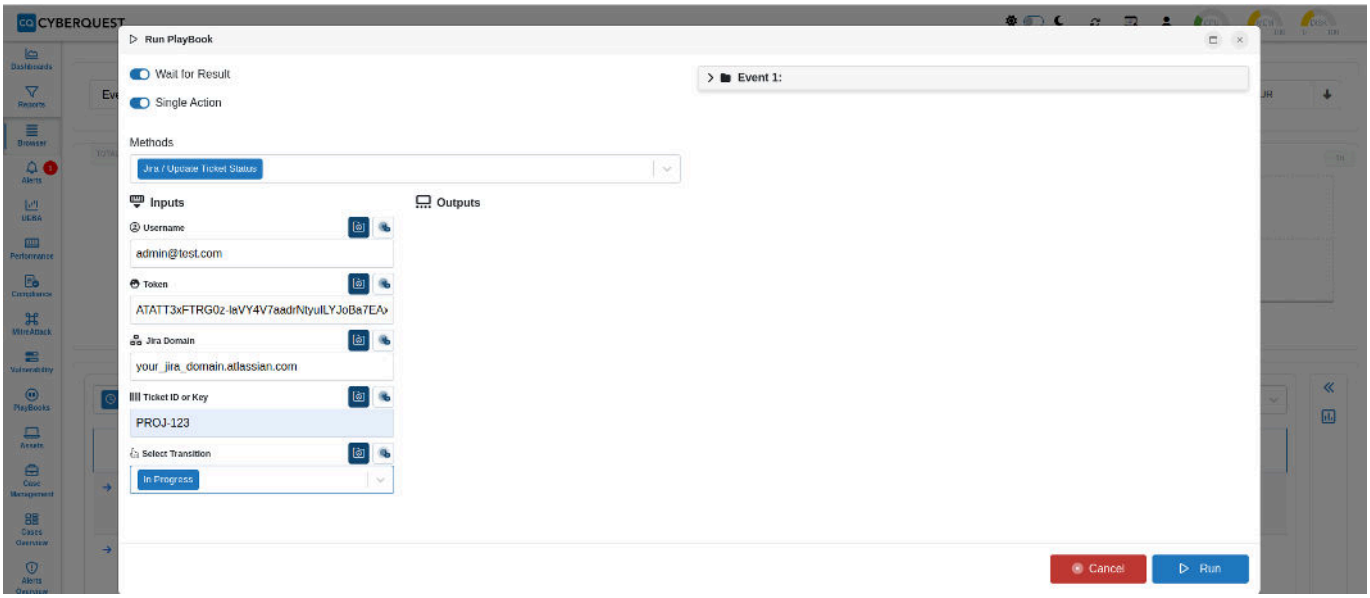
Returns either all transitions or a transition that can be performed by the user on an issue, based on the issue status.



Inputs	Description
Username (is required)	Your account has a username set up to access the Jira server
Token(is required)	Your account has an API token to access the Jira server
Jira Domain (is required)	Your Jira domain(ex: your_jira_domain.atlassian.com)
Ticket ID or Key (is required)	The ID or key of the issue.

Jira/Update Ticket Status

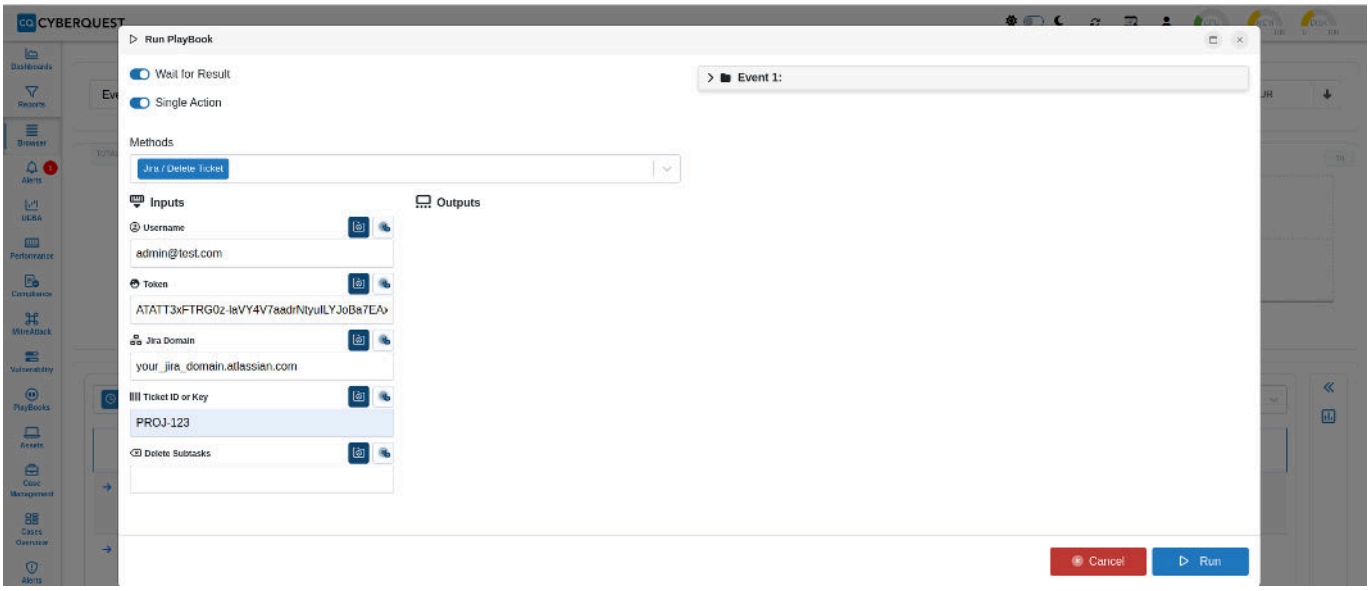
Performs an issue transition and, if the transition has a screen, updates the fields from the transition screen.



Inputs	Description
Username (is required)	Your account has a username set up to access the Jira server
Token(is required)	Your account has an API token to access the Jira server
Jira Domain (is required)	Your Jira domain(ex: your_jira_domain.atlassian.com)
Ticket ID or Key (is required)	The ID or key of the issue.
Select Transition (is required)	The ID of the issue transition.

Jira/Delete Ticket

An issue cannot be deleted if it has one or more subtasks. To delete an issue with subtasks, set deleteSubtasks. This causes the issue subtasks to be deleted with the issue.

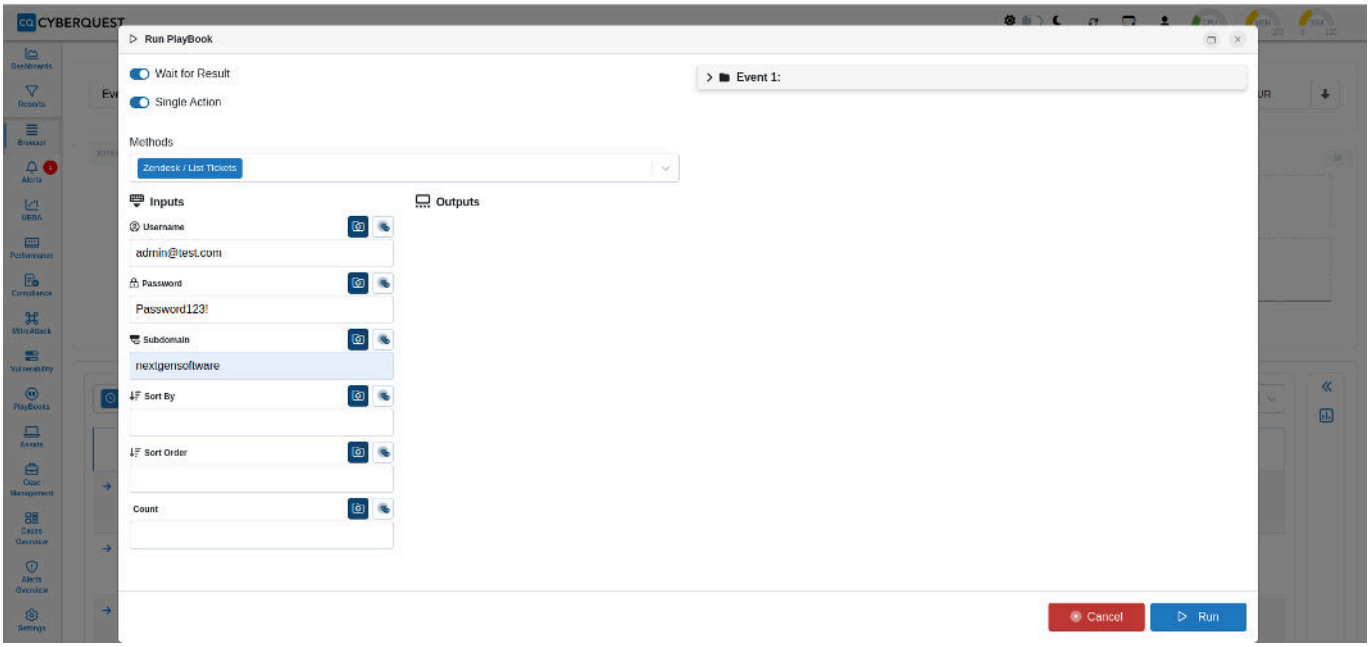


Inputs	Description
Username (is required)	Your account has a username set up to access the Jira server
Token(is required)	Your account has an API token to access the Jira server
Jira Domain (is required)	Your Jira domain(ex: your_jira_domain.atlassian.com)
Ticket ID or Key (is required)	The ID or key of the issue.
Delete Subtasks	“Whether the issue subtasks are deleted when the issue is deleted.Default: false”. Valid values: true, false

Zendesk

Zendesk/List Tickets

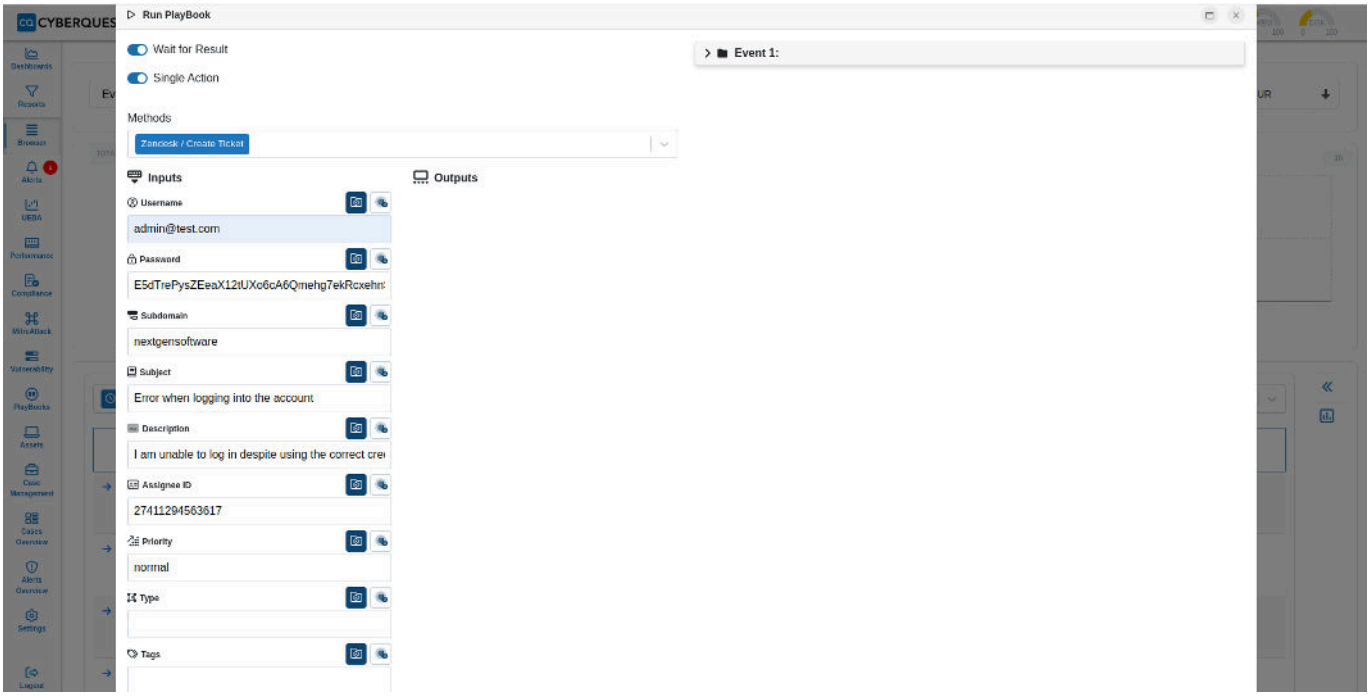
Retrieve a comprehensive list of all tickets from Zendesk.



Inputs	Description
Username (is required)	The username from the account created on Zendesk
Password (is required)	The API token generated from Admin Page
Subdomain (is required)	The subdomain created using zendesk, for example: nextgensoftware.
Sort By	Possible values are assignee, assignee.name, created_at, group, id, requester, requester.name, status, subject, updated_at
Sort Order	One of asc, desc. Defaults to asc
Count	Number of tickets that you want to fetch from Zendesk per page

Zendesk/Create Ticket

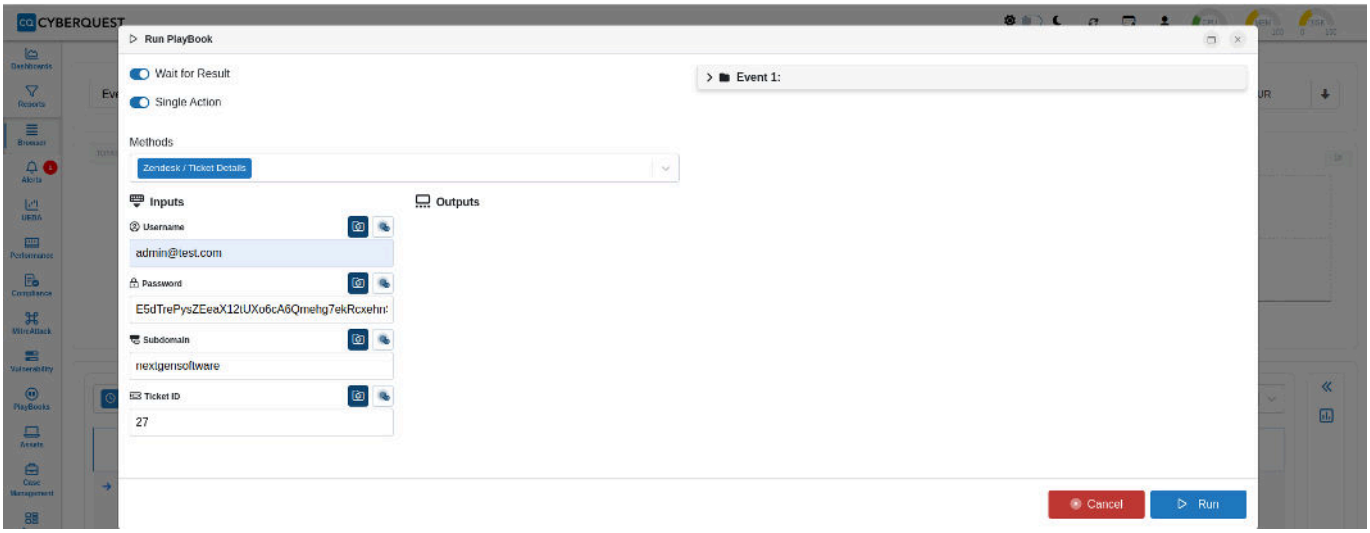
Build a new ticket in Zendesk using the supplied subject, assignee ID, description, and optional parameters.



Inputs	Description
Username (is required)	The username from the account created on Zendesk
Password (is required)	The API token generated from Admin Page
Subdomain (is required)	The subdomain created using zendesk, for example: nextgensoftware.
Subject	Provide the subject of the ticket
Description (is required)	Give a full explanation of the ticket you would like to create in Zendesk.
Assignee ID (is required)	Specify the ID of the person who should handle this ticket
Priority	Indicate the importance of this ticket by choosing a priority: Low, Normal, High, or Urgent.
Type	Classify the ticket as a Question, Incident, Problem, or Task
Tags	Enter a comma-separated list of tags to apply to the ticket

Zendesk/Ticket Details

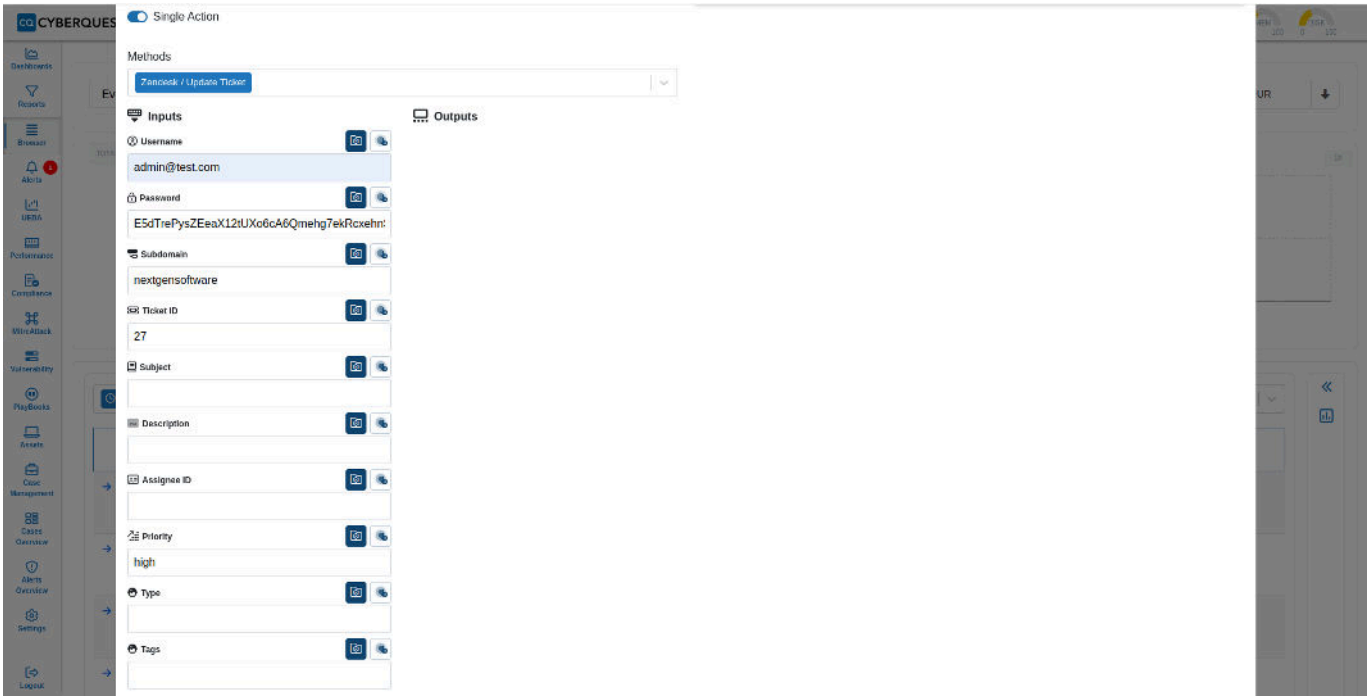
Obtain detailed ticket data based on provided ticket ID.



Inputs	Description
Username (is required)	The username from the account created on Zendesk
Password (is required)	The API token generated from Admin Page
Subdomain (is required)	The subdomain created using zendesk, for example: nextgensoftware.
Ticket ID (is required)	Enter the ticket id to retrieve its details.

Zendesk/Update Ticket

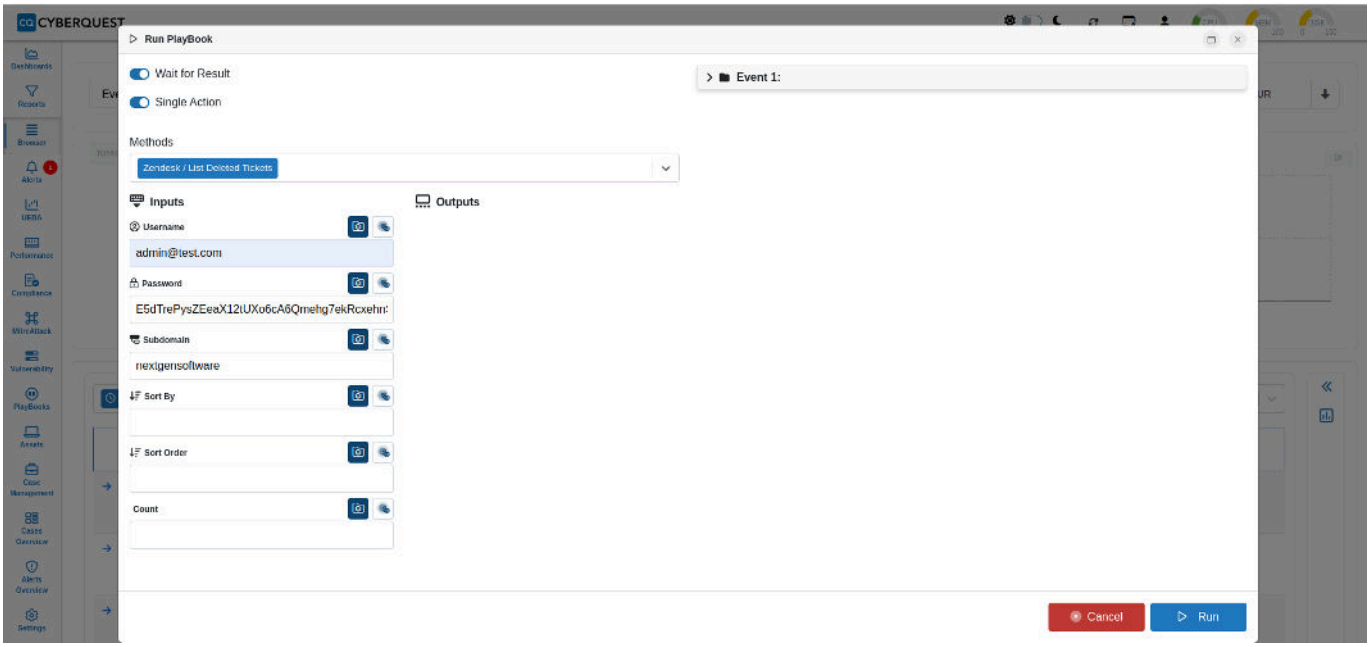
Make changes to a specific ticket based on provided information.



Inputs	Description
Username (is required)	The username from the account created on Zendesk
Password (is required)	The API token generated from Admin Page
Subdomain (is required)	The subdomain created using zendesk, for example: nextgensoftware.
Subject	Provide the subject of the ticket
Description	Give a full explanation of the ticket you would like to create in Zendesk.
Assignee ID	Specify the ID of the person who should handle this ticket
Priority	Indicate the importance of this ticket by choosing a priority: Low, Normal, High, or Urgent.
Type	Classify the ticket as a Question, Incident, Problem, or Task
Tags	Enter a comma-separated list of tags to apply to the ticket

Zendesk/List Deleted Tickets

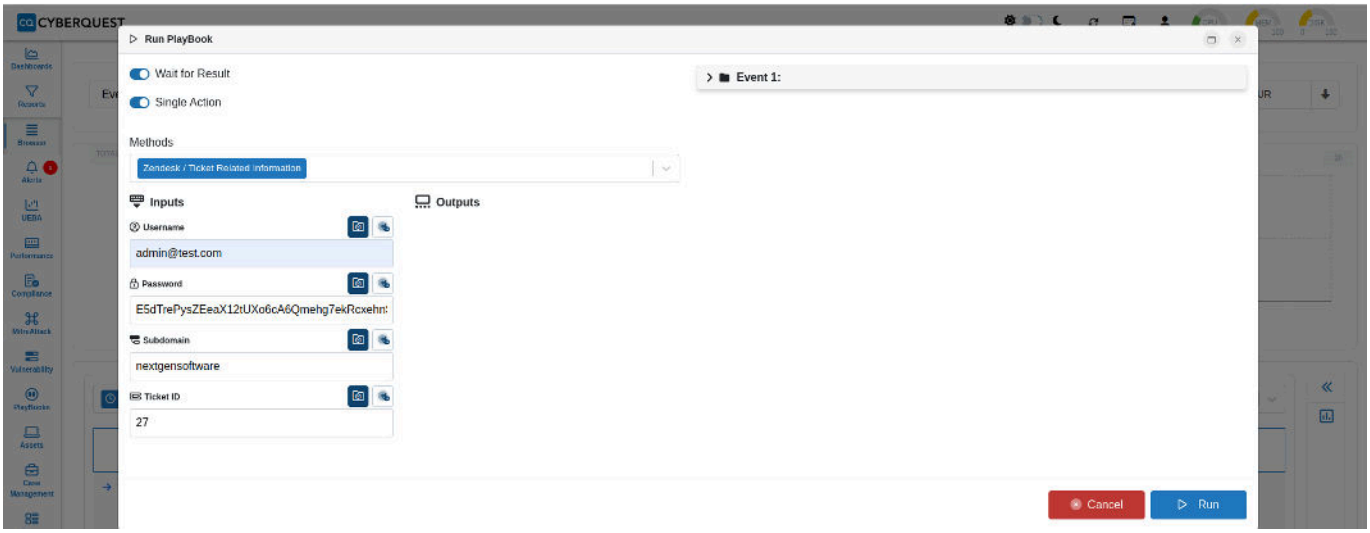
Retrieve up to 100 deleted tickets per page, excluding those permanently removed.



Inputs	Description
Username (is required)	The username from the account created on Zendesk
Password (is required)	The API token generated from Admin Page
Subdomain (is required)	The subdomain created using zendesk, for example: nextgensoftware.
Sort By	Possible values are assignee, assignee.name, created_at, group, id, requester, requester.name, status, subject, updated_at
Sort Order	One of asc, desc. Defaults to asc
Count	Number of tickets that you want to fetch from Zendesk per page

Zendesk/Ticket Related Information

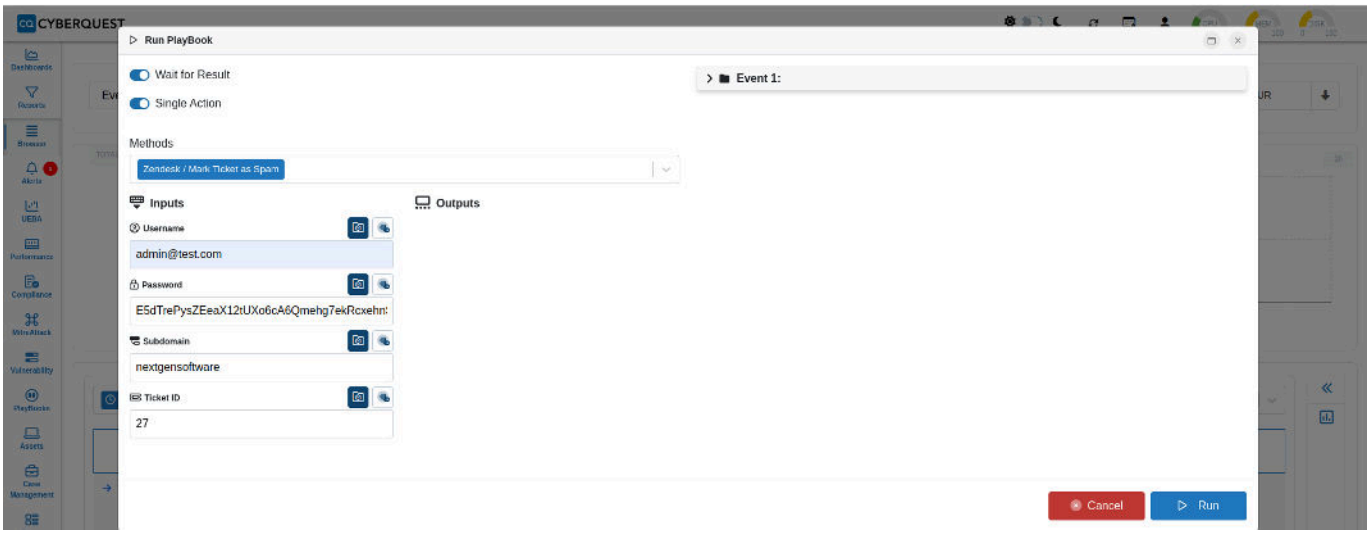
Retrieve associated data for a specific ticket.



Inputs	Description
Username (is required)	The username from the account created on Zendesk
Password (is required)	The API token generated from Admin Page
Subdomain (is required)	The subdomain created using zendesk, for example: nextgensoftware.
Ticket ID (is required)	Enter the ticket id to retrieve its details.

Zendesk/Mark Ticket as Spam

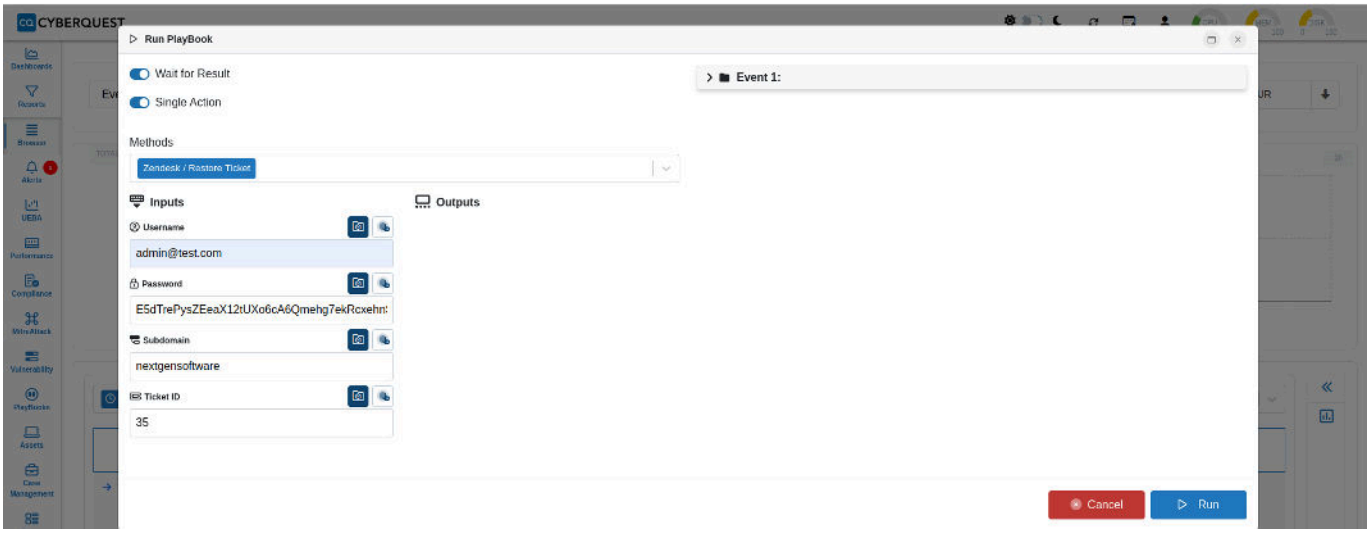
Indicate a ticket as spam in the Zendesk system.



Inputs	Description
Username (is required)	The username from the account created on Zendesk
Password (is required)	The API token generated from Admin Page
Subdomain (is required)	The subdomain created using zendesk, for example: nextgensoftware.
Ticket ID (is required)	Please provide the ID of the ticket you want to flag as spam

Zendesk/Restore Ticket

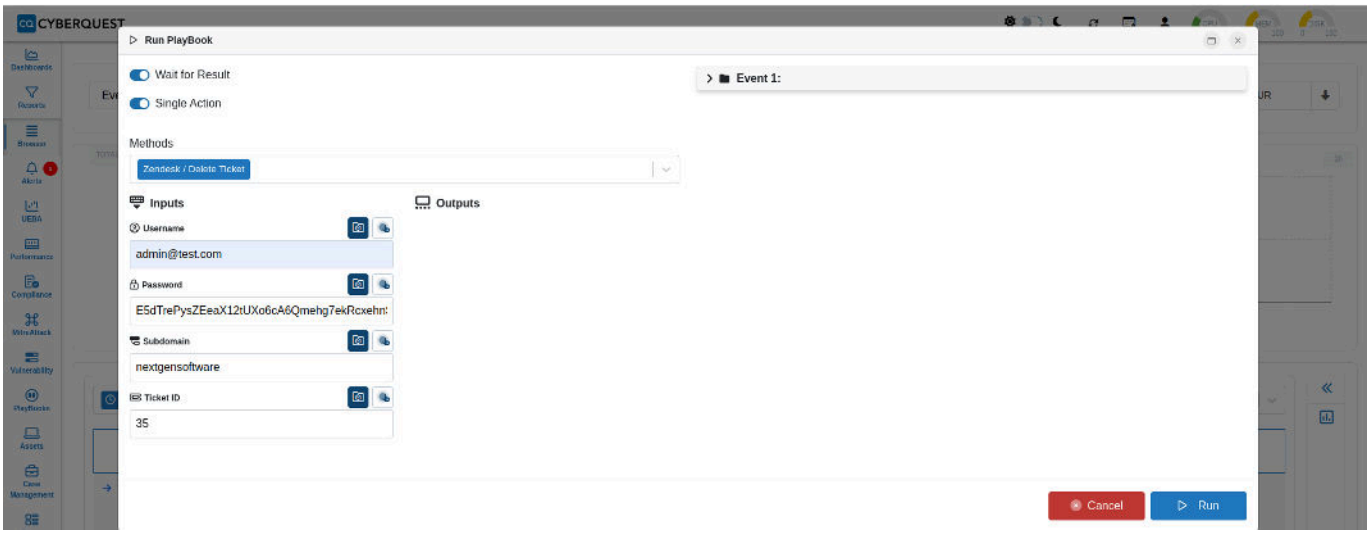
Bring back a previously deleted ticket.



Inputs	Description
Username (is required)	The username from the account created on Zendesk
Password (is required)	The API token generated from Admin Page
Subdomain (is required)	The subdomain created using zendesk, for example: nextgensoftware.
Ticket ID (is required)	Enter the number of the deleted ticket you wish to recover

Zendesk/Delete Ticket

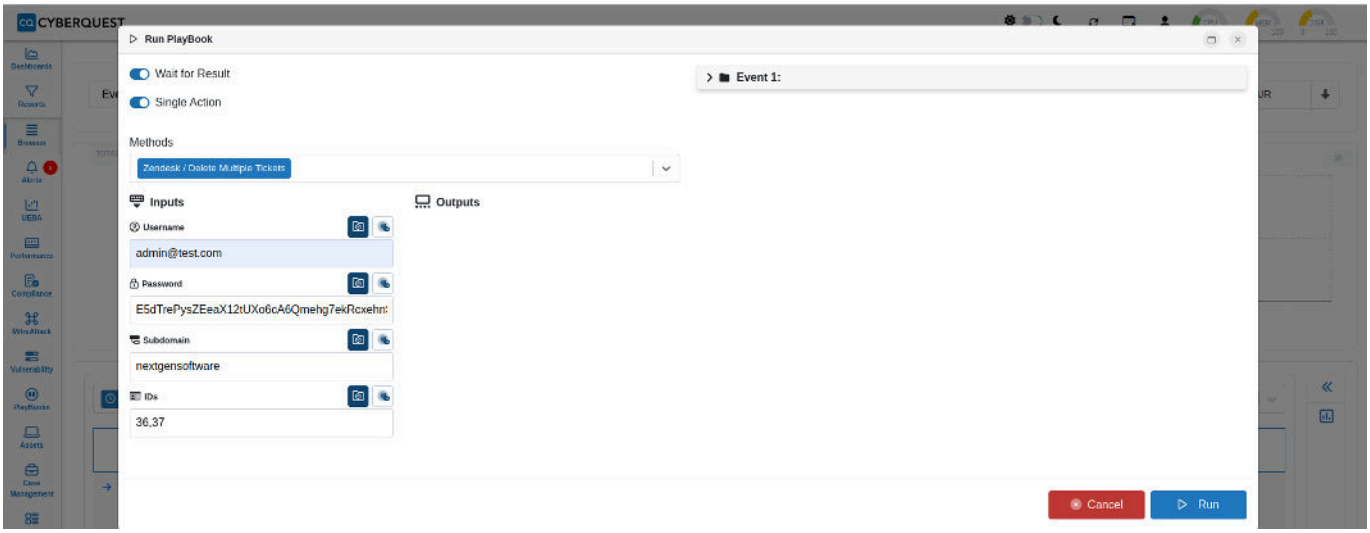
Remove a ticket from Zendesk (recoverable for 30 days).



Inputs	Description
Username (is required)	The username from the account created on Zendesk
Password (is required)	The API token generated from Admin Page
Subdomain (is required)	The subdomain created using zendesk, for example: nextgensoftware.
Ticket ID (is required)	Please provide the ID of the ticket you want to delete

Zendesk/Delete Ticket Permanently

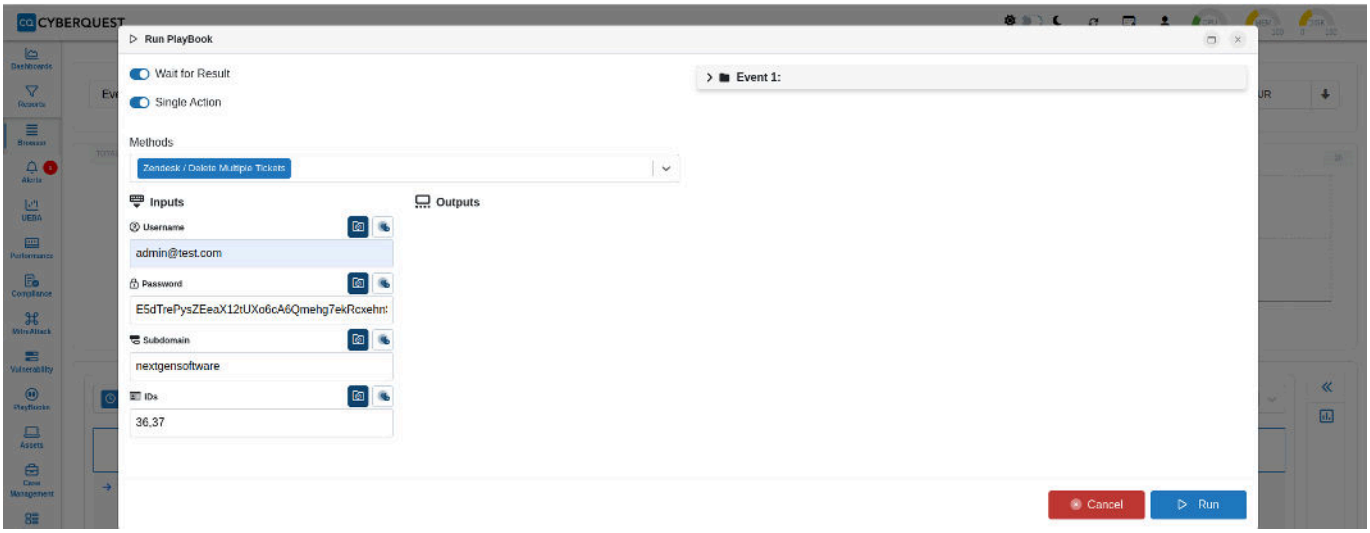
Completely remove a previously deleted ticket.



Inputs	Description
Username (is required)	The username from the account created on Zendesk
Password (is required)	The API token generated from Admin Page
Subdomain (is required)	The subdomain created using zendesk, for example: nextgensoftware.
Ticket ID (is required)	“Enter the number of the ticket you wish to delete completely.The Delete Ticket method must be used first, after that this method will work

Zendesk/Delete Multiple Tickets

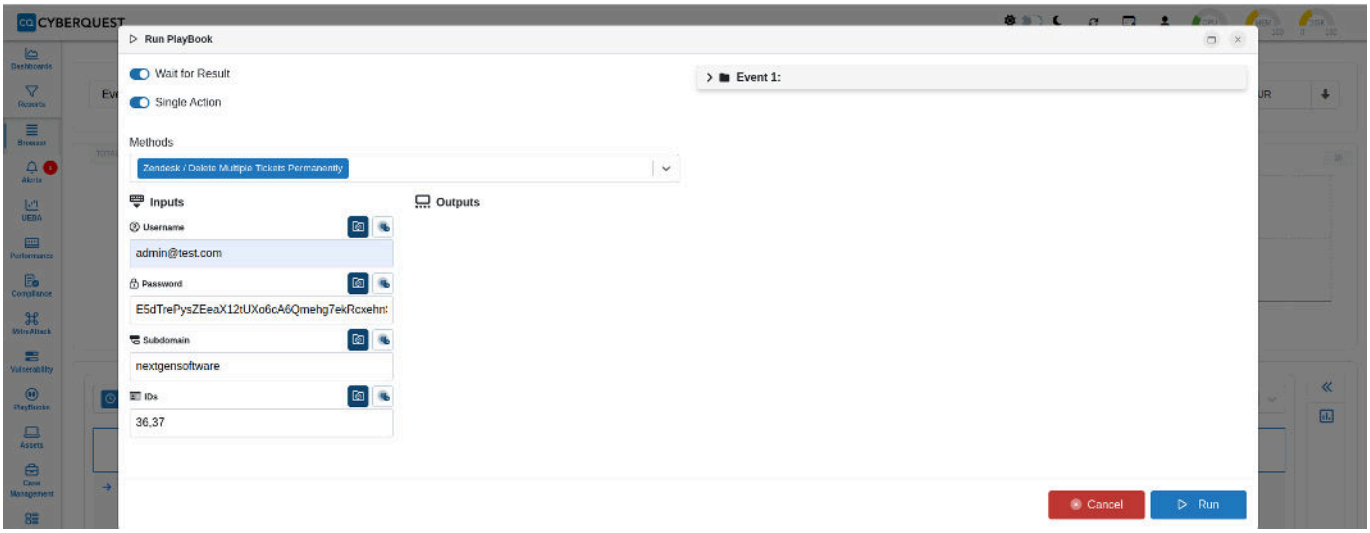
Delete multiple tickets. Maximum 100 IDs.



Inputs	Description
Username (is required)	The username from the account created on Zendesk
Password (is required)	The API token generated from Admin Page
Subdomain (is required)	The subdomain created using zendesk, for example: nextgensoftware.
IDs (is required)	Please input a CSV or list of up to 100 ticket IDs to be deleted.

Zendesk/Delete Multiple Tickets Permanently

Permanently erase up to 100 previously deleted tickets.



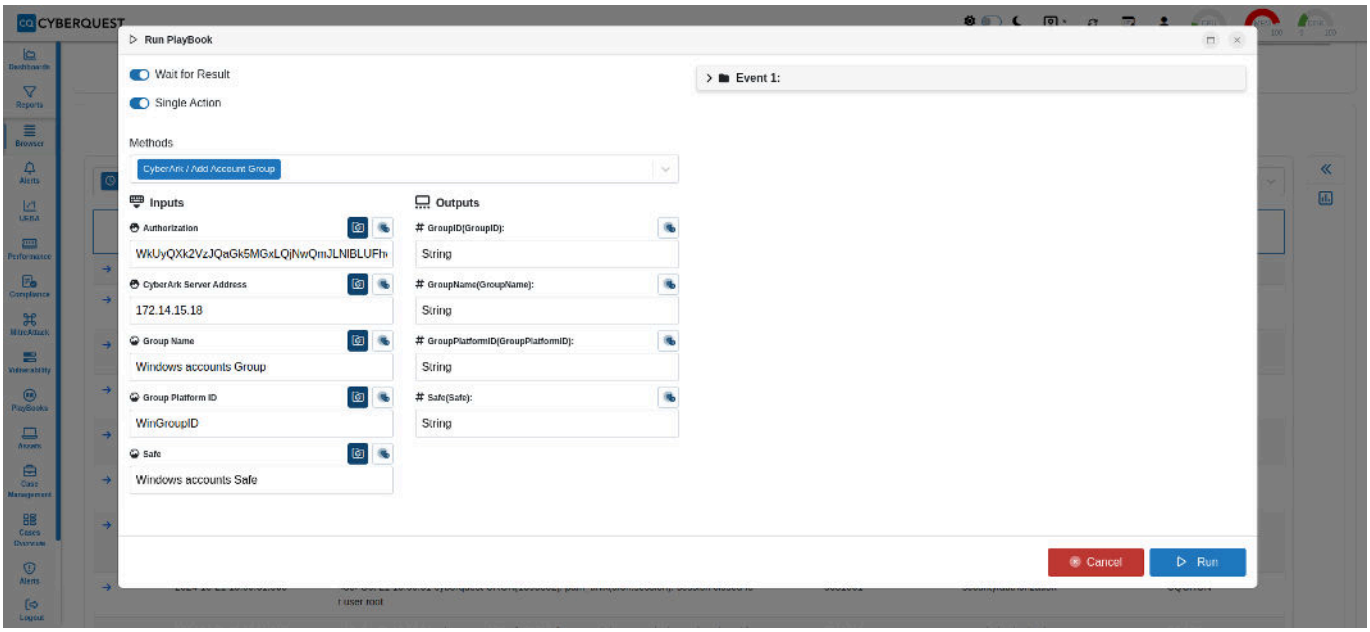
Inputs	Description
Username (is required)	The username from the account created on Zendesk
Password (is required)	The API token generated from Admin Page
Subdomain (is required)	The subdomain created using zendesk, for example: nextgensoftware.
IDs (is required)	Please input a CSV or list of up to 100 ticket IDs to be deleted permanently

CyberArk

CyberArk/Add Account Group

This method enables application managers to define a new account group automatically, and manage accounts as part of a group.To create an account group, users require the following permissions in the Safe where the group is created:

- Add accounts
- Update account content
- Update account properties
- Create folders

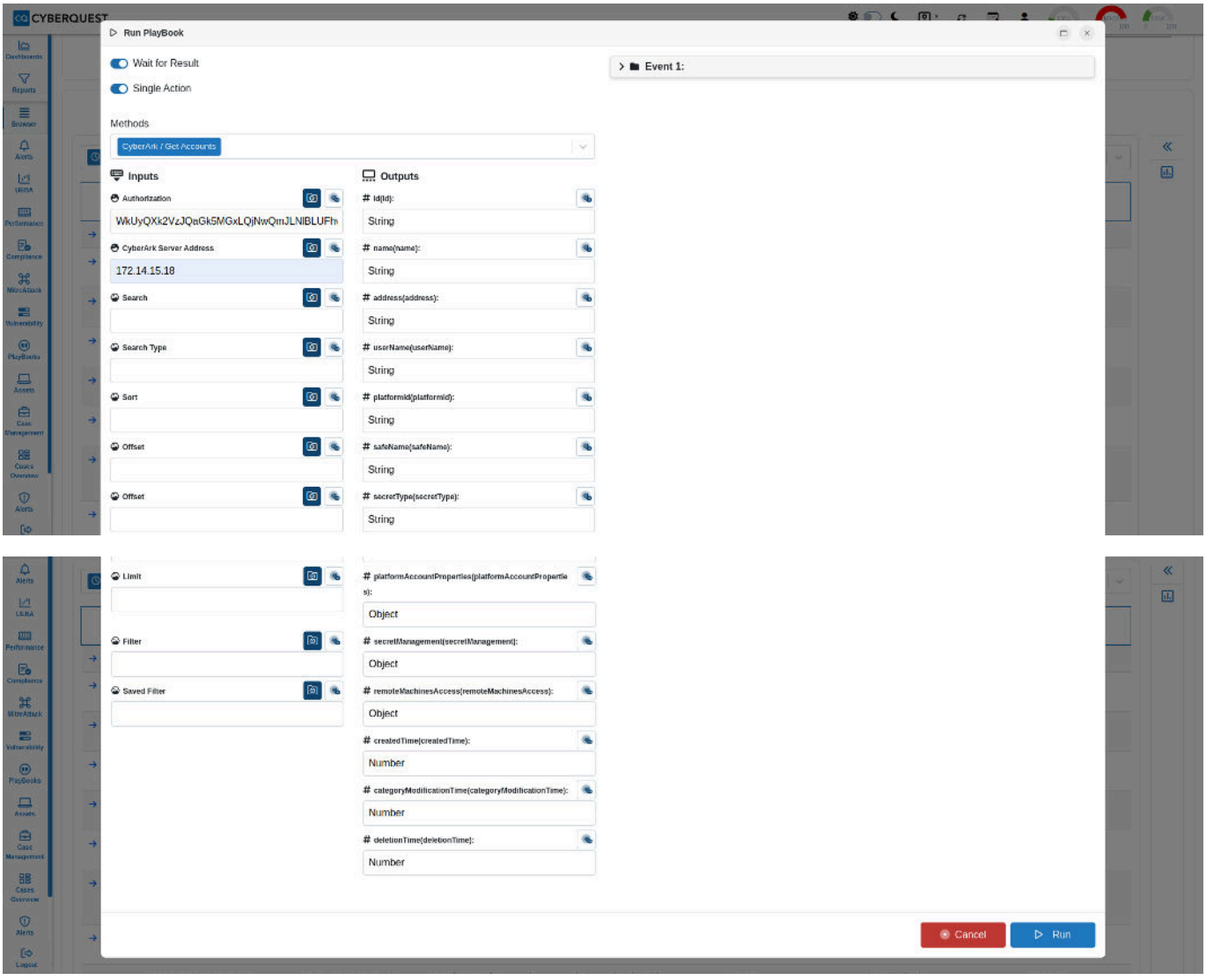


Inputs	Description
Authorization (is required)	The token that identifies the session, encoded in BASE 64.
CyberArk Server Address (is required)	The address of the CyberArk Server
Group Name (is required)	The name of the newly created group
Group Platform ID (is required)	The name of the platform of the group.The associated platform must be set to PolicyType=Group OR Rotational Group
Safe (is required)	The name of the Safe where the group will be created

Outputs	Description
GroupID (GroupID)	The ID of the newly created group
GroupName(GroupName)	The name of the newly created group
GroupPlatformID(GroupPlatformID)	The ID of the platform associated with the group
Safe(Safe)	The name of the Safe where the group exists

CyberArk/Get Accounts

This method returns a list of all the accounts in the Vault.

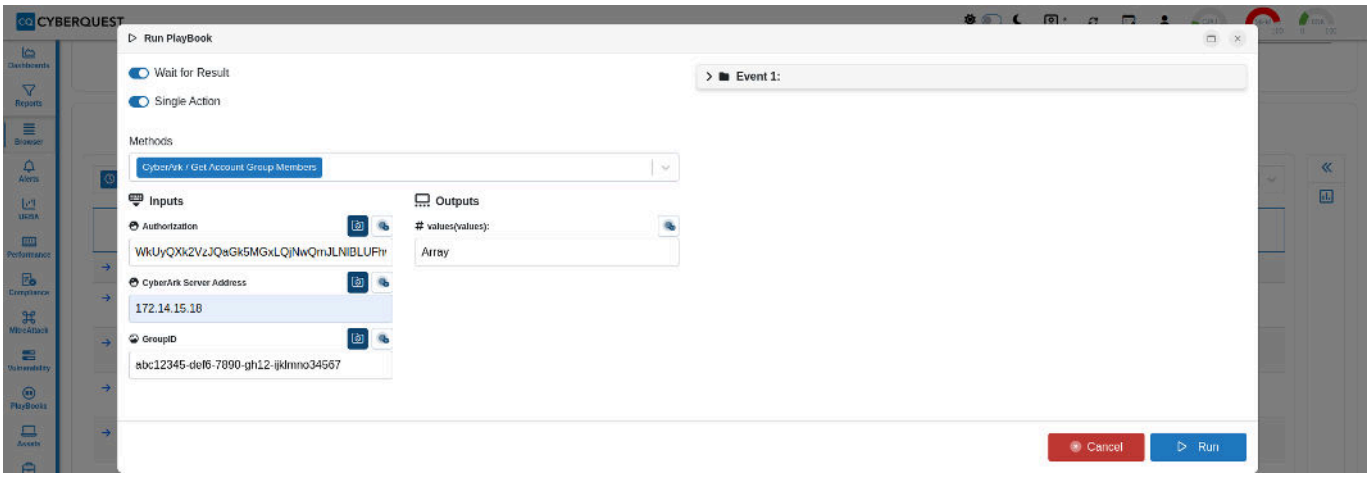


Inputs	Description
Authorization (is required)	The token that identifies the session, encoded in BASE 64
CyberArk Server Address (is required)	The address of the CyberArk Server
Search	A list of keywords to search for in accounts, separated by a space
Search Type	Get accounts that either contain or start with the value specified in the Search parameter
Sort	The property or properties that you want to sort returned accounts, followed by asc (default) or desc to control sort direction. Separate multiple properties with commas, up to a maximum of three properties
Offset	Offset of the first account that is returned in the collection of results
Limit	The maximum number of returned accounts. The maximum number that you can specify is 1000. When used together with the Offset parameter, this value determines the number of accounts to return, starting from the first account that is returned
Filter	The maximum number of returned accounts. The maximum number that you can specify is 1000. When used together with the Offset parameter, this value determines the number of accounts to return, starting from the first account that is returned
Saved Filter	Search for accounts using a saved filter(s).

Outputs	Description
id (id)	The unique ID of the account
name(name)	The unique name of the Safe where the account is located
address(address)	The name or address of the machine where the account is used
userName(userName)	The account user name
platformId(platformId)	The platform assigned to the account
safeName(safeName)	safeName
secretType(secretType)	The unique name of the Safe where the account is located
platformAccountProperties(platformAccountProperties)	The object containing key-value pairs to associate with the account, as defined by the account platform. Optional properties that do not exist for the account will not be returned here, and internal properties are not returned
secretManagement(secretManagement)	Additional management parameters
remoteMachinesAccess(remoteMachinesAccess)	Additional remote access machines
createdTime(createdTime)	The date and time the account was created
categoryModificationTime(categoryModificationTime)	The last time the account or one of its file categories was created or changed
deletionTime(deletionTime)	The last time the account or one of its file categories was created or changed

CyberArk/Get Account Group Members

This method returns all the members of an existing account group. These accounts can be either password accounts or SSH Key accounts.

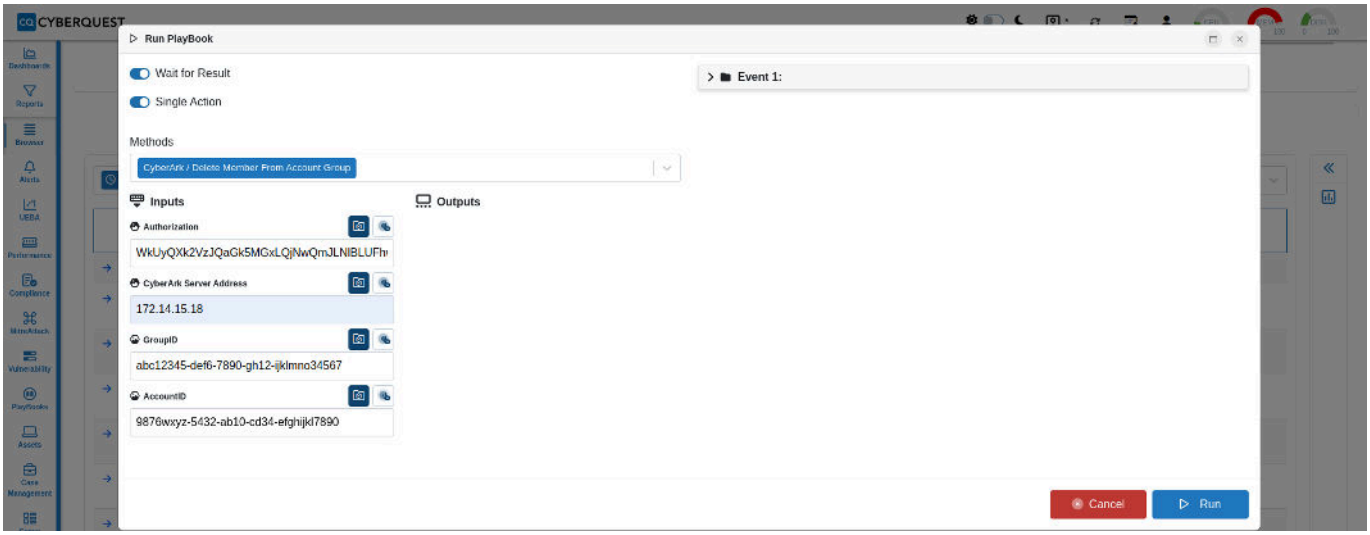


Inputs	Description
Authorization (is required)	The token that identifies the session, encoded in BASE 64
CyberArk Server Address (is required)	The address of the CyberArk Server
GroupID (is required)	The unique ID of the group

Outputs	Description
ARRAY_VALUES_KEY(ARRAY_VALUES_KEY)	The list of accounts

CyberArk/Delete Member From Account Group

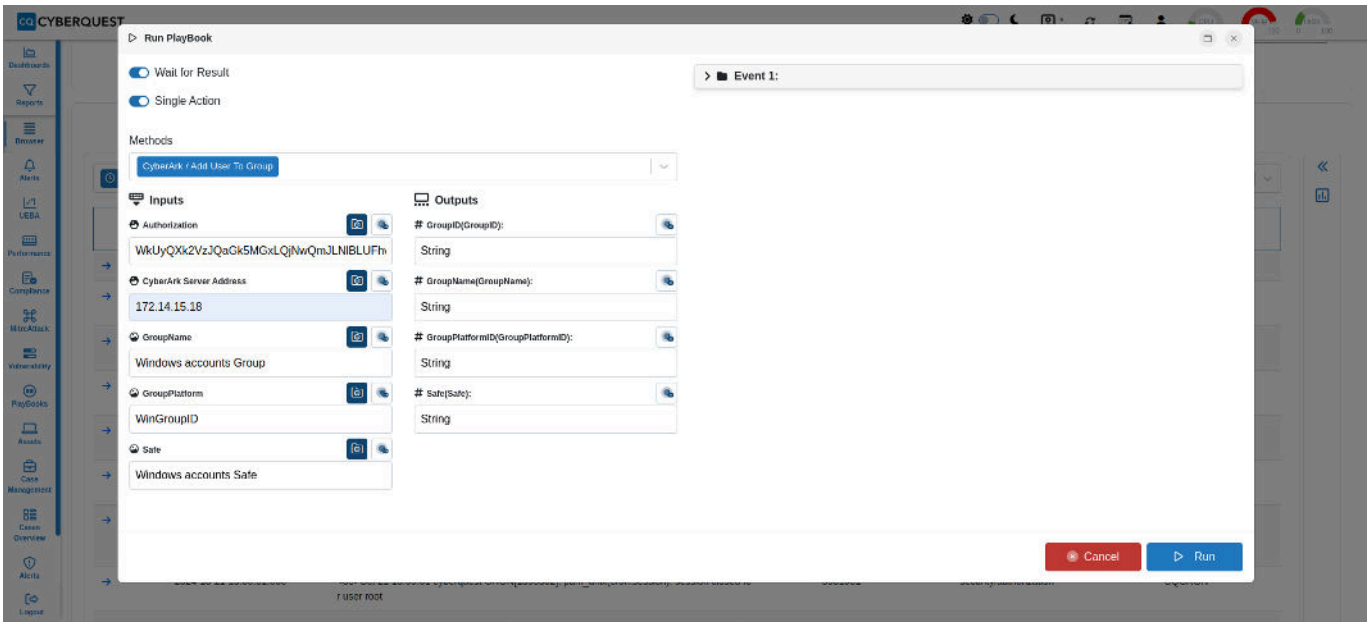
This method removes an account member from an account group. This account can be either a password account or an SSH Key account.



Inputs	Description
Authorization (is required)	The token that identifies the session, encoded in BASE 64
CyberArk Server Address (is required)	The address of the CyberArk Server
GroupID (is required)	The unique ID of the group
AccountID (is required)	The unique ID of the account

CyberArk/Add User To Group

This method enables application managers to define a new account group automatically, and manage accounts as part of a group.

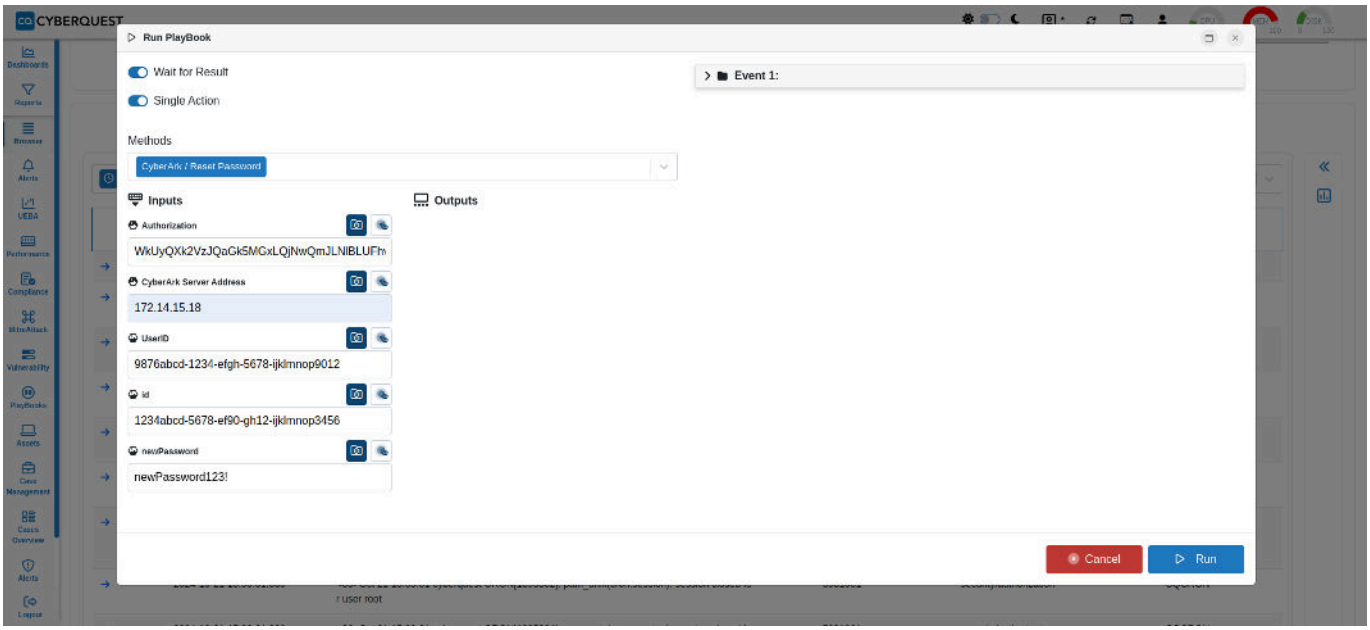


Inputs	Description
Authorization (is required)	The token that identifies the session, encoded in BASE 64
CyberArk Server Address (is required)	The address of the CyberArk Server
GroupName (is required)	The name of the newly created group
GroupPlatform (is required)	The name of the platform of the group. The associated platform must be set to PolicyType=Group OR Rotational Group
Safe (is required)	The name of the Safe where the group will be created

Outputs	Description
GroupID (GroupID)	The ID of the newly created group
GroupName(GroupName)	The name of the newly created group
GroupPlatformID(GroupPlatformID)	The ID of the platform associated with the group
Safe(Safe)	The name of the Safe where the group exists

CyberArk/Reset Password

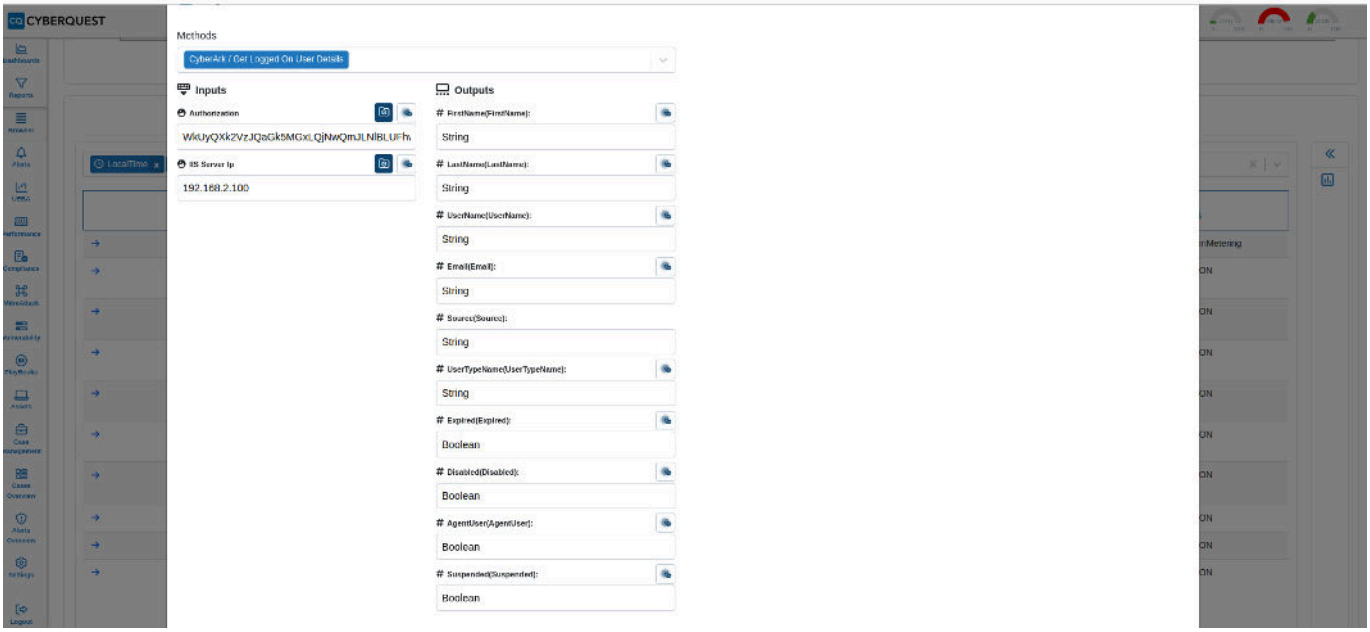
This method resets an existing Vault users password.



Inputs	Description
Authorization (is required)	The token that identifies the session, encoded in BASE 64
CyberArk Server Address (is required)	The address of the CyberArk Server
UserID (is required)	The ID of the account to which the password will be generated
id (is required)	The users unique ID
newPassword (is required)	The user's new password

CyberArk/Get Logged On User Details

This method returns user information of the user who is logged on.

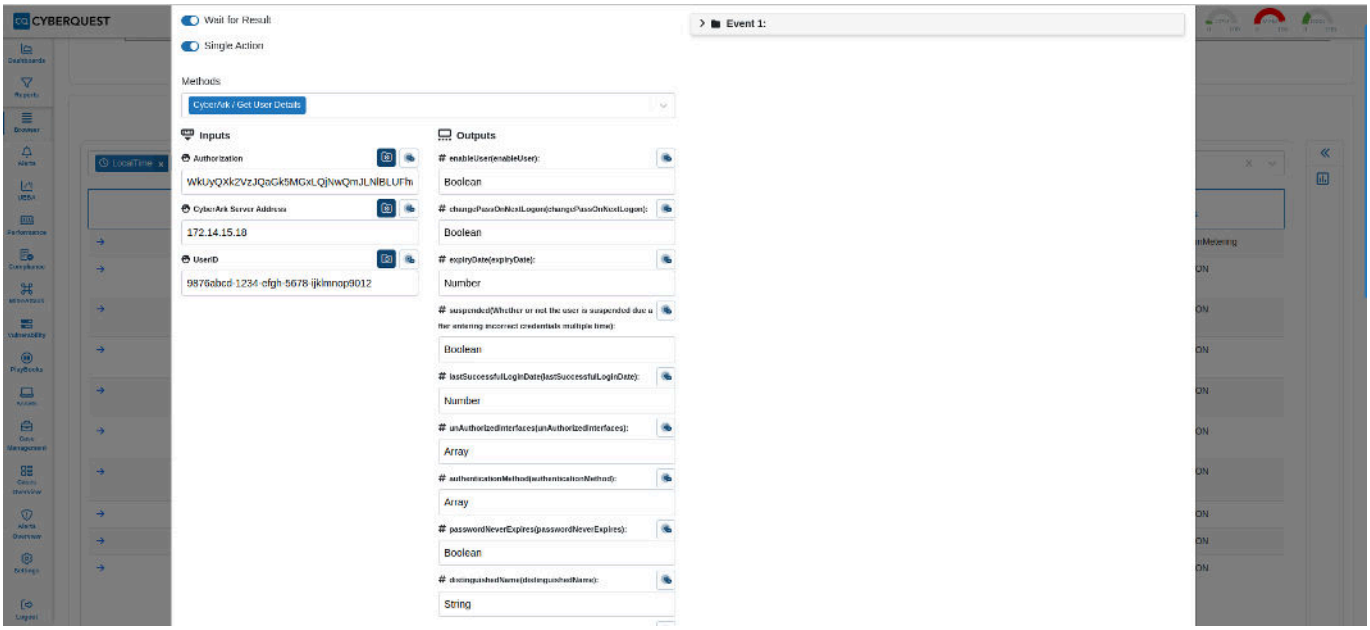


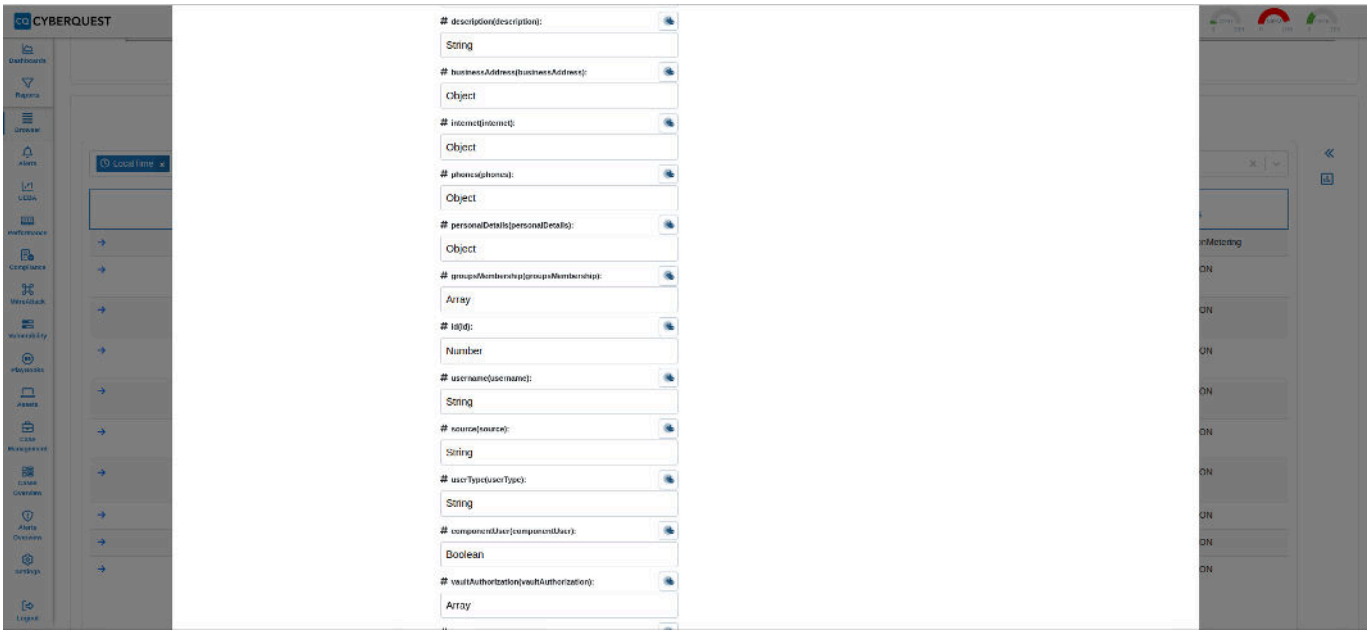
Inputs	Description
Authorization (is required)	The token that identifies the session, encoded in BASE 64
IIS Server Ip (is required)	The address of the IIS Server

Outputs	Description
FirstName (FirstName)	The First Name of the user
LastName(LastName)	The Last Name of the user
UserName(UserName)	The UserName of the user
Email(Email)	The Email address of the user
Source(Source)	
UserTypeName(UserTypeName)	The Type of the user
Expired(Expired)	True if the user is expired, otherwise false
Disabled(Disabled)	True if the user is disabled, otherwise false
AgentUser(AgentUser)	True if the user is agent, otherwise false
Suspended(Suspended)	True if the user is suspended, otherwise false

CyberArk/Get User Details

This method returns information about a specific user in the Vault.



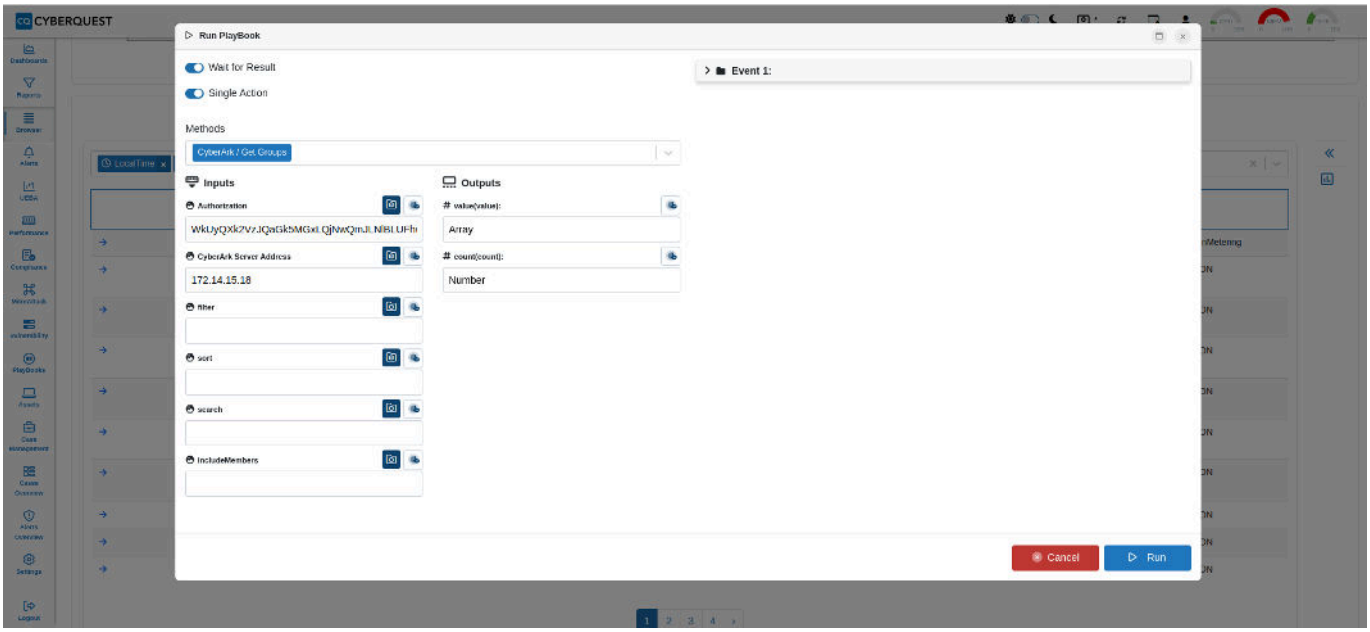


Inputs	Description
Authorization (is required)	The token that identifies the session, encoded in BASE 64
CyberArk Server Address (is required)	The address of the CyberArk Server
UserID (is required)	The ID of the user for which information is returned

Outputs	Description
enableUser (enableUser)	Whether or not the user is enabled
changePassOnNextLogon(changePassOnNextLogon)	Whether or not the user must change their password from the second log on onward
expiryDate(expiryDate)	The date when the user expires
suspended(suspended)	Whether or not the user is suspended due after entering incorrect credentials multiple time
lastSuccessfulLoginDate(lastSuccessfulLoginDate)	The date that the user last logged on to the Vault successfully
unAuthorizedInterfaces(unAuthorizedInterfaces)	The CyberArk interfaces that this user is not authorized to use. The possible values depend on the specific user type as defined in the license
authenticationMethod(authenticationMethod)	The authentication method that the user uses to log on
passwordNeverExpires(passwordNeverExpires)	Whether the user's password is retained until the user changes it.
distinguishedName(distinguishedName)	The user's distinguished name. The usage is for PKI authentication, this will match the certificate Subject Name or domain name
description(description)	Notes and comments
businessAddress(businessAddress)	The user's postal address, including:City, state, zip, and country Street
internet(internet)	The users email addresses, including: Home page, Home email, Business email, Other email
phones(phones)	phones
personalDetails(personalDetails)	The users personal details, including: firstName, middleName, lastName, address, city, state, zip, country, title, organization, department, profession
groupsMembership(groupsMembership)	List of groups in which the user is a member
id(id)	The unique ID of the user
username(username)	The name of the user
source(source)	The source of the user
userType(userType)	The user type as defined in the license
componentUser(componentUser)	Whether the user is a known component or not. If the user is a component, the value is true. Otherwise, its false
vaultAuthorization(vaultAuthorization)	The user permissions
location(location)	The location in the Vault where the user will be created

CyberArk/Get Groups

This method returns a list of all existing user groups.

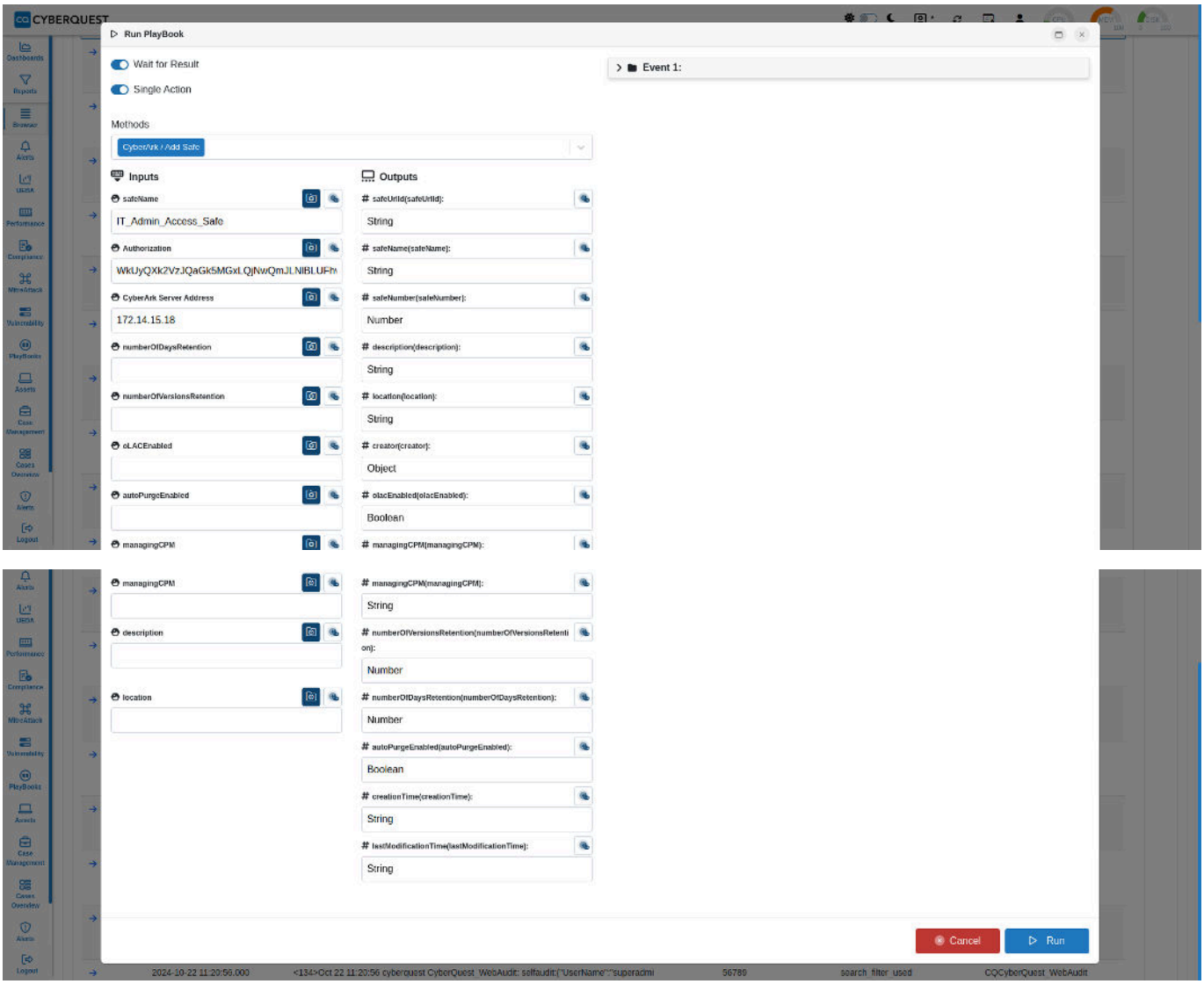


Inputs	Description
Authorization (is required)	The token that identifies the session, encoded in BASE 64
CyberArk Server Address (is required)	The address of the CyberArk Server
filter	Filters according to the REST standard
sort	Property or properties by which to sort returned users, followed by asc (default) or desc to control sort direction. Separate multiple properties with commas, up to a maximum of three properties: groupname, directory, location
search	Searches according to the REST standard (searching with contains). Search matches when all search terms appear in the group name
includeMembers	Whether or not to return members for each user group as part of the response. If not sent, the value will be False

Outputs	Description
value (value)	The list of groups
count(count)	The number of groups

CyberArk/Add Safe

This method adds a new Safe to the Vault.

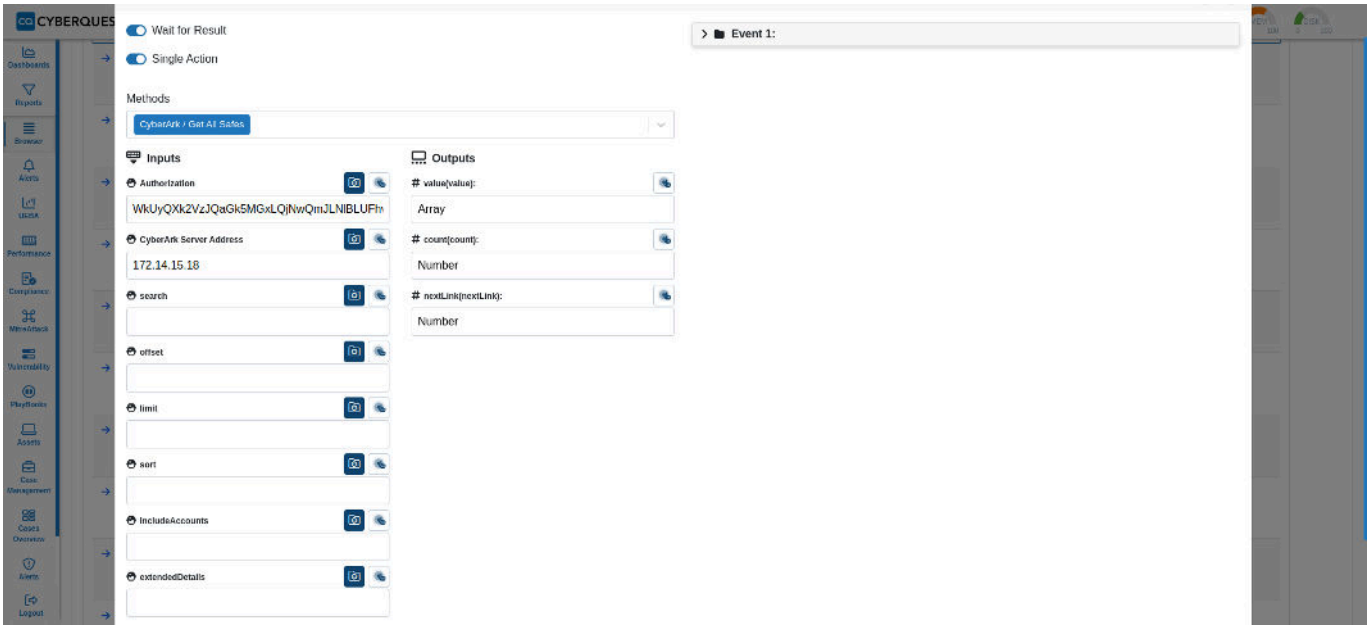


Inputs	Description
safeName (is required)	The unique name of the Safe
Authorization (is required)	The token that identifies the session, encoded in BASE 64
CyberArk Server Address (is required)	The address of the CyberArk Server
numberOfDaysRetention	The number of days that password versions are saved in the Safe
numberOfVersionsRetention	The number of retained versions of every password that is stored in the Safe
oLACEnabled	Whether or not to enable Object Level Access Control for the new Safe.
autoPurgeEnabled	Whether or not to automatically purge files after the end of the Object History Retention Period defined in the Safe properties. Report Safes and PSM Recording Safes are created automatically with AutoPurgeEnabled set to Yes. These Safes cannot be managed by the CPM
managingCPM	The name of the CPM user who will manage the new Safe
description	The description of the Safe
location	The location of the Safe in the Vault

Outputs	Description
safeUrlId (safeUrlId)	The unique ID of the Safe used when calling Safe APIs
safeName(safeName)	The name of the Safe
safeNumber(safeNumber)	The unique numerical ID of the Safe
description(description)	The description of the Safe
location(location)	The location of the Safe in the Vault
creator(creator)	Contains the following parameters: creator.id: The ID of the user that created the Safe. Type: String, creator.name: The name of the user that created the Safe
olacEnabled(olacEnabled)	Whether or not to enable Object Level Access Control for the new Safe
managingCPM(managingCPM)	The name of the CPM user who will manage the new Safe
numberOfVersionsRetention(numberOfVersionsRetention)	The number of retained versions of every password that is stored in the Safe
numberOfDaysRetention(numberOfDaysRetention)	The number of days that password versions are saved in the Safe
autoPurgeEnabled(autoPurgeEnabled)	Whether or not to automatically purge files after the end of the Object History Retention Period defined in the Safe properties. Report Safes and PSM Recording Safes are created automatically with AutoPurgeEnabled set to Yes. In addition, these Safes cannot be managed by the CPM
creationTime(creationTime)	The Unix creation time of the Safe
lastModificationTime(lastModificationTime)	The Unix time when the Safe was last updated

CyberArk/Get All Safes

This method returns a list of all Safes in the Vault that the user has permissions for.

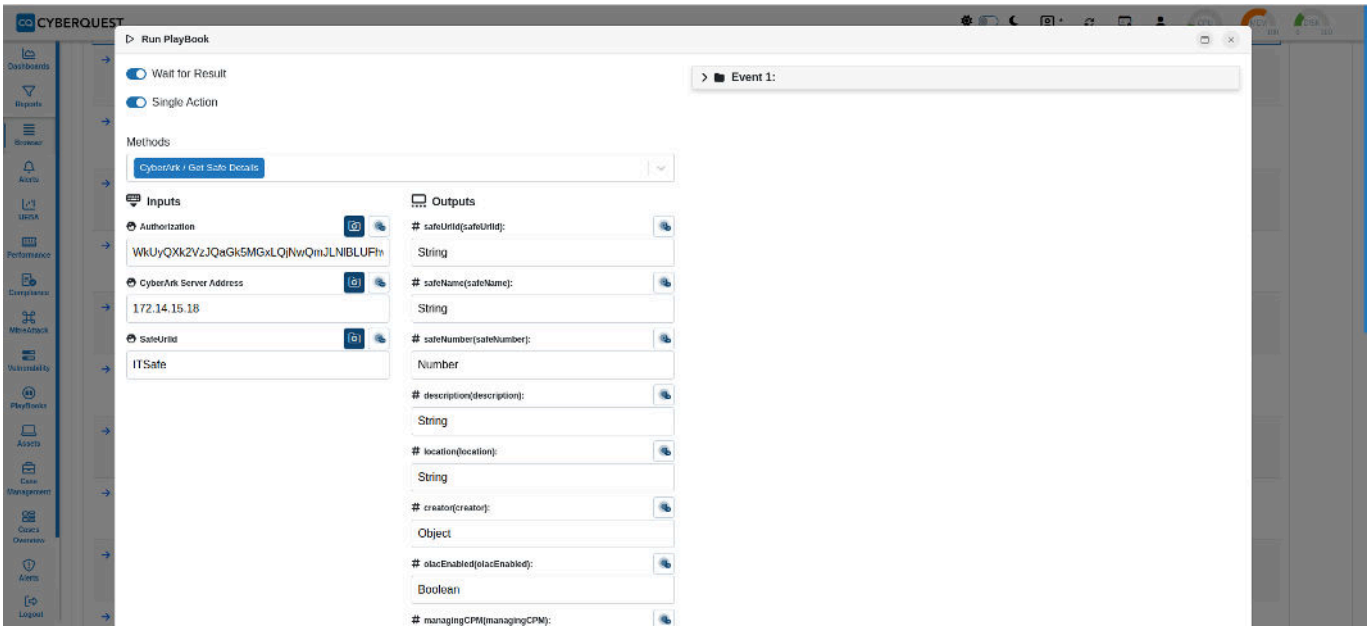


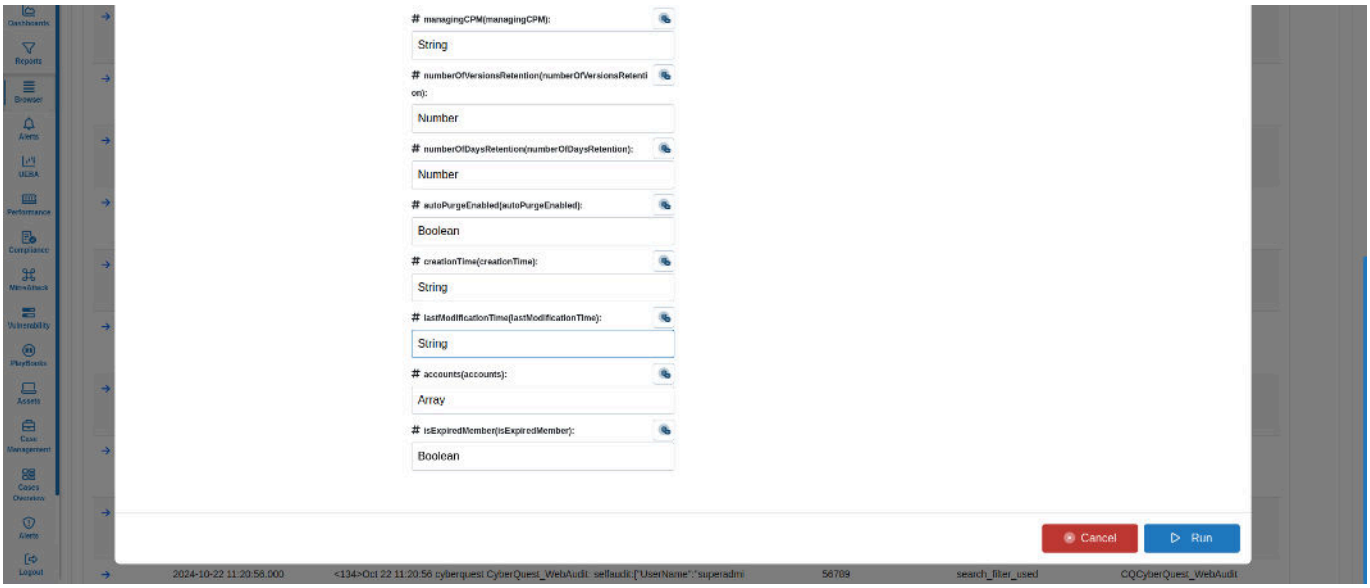
Inputs	Description
Authorization (is required)	The token that identifies the session, encoded in BASE 64
CyberArk Server Address (is required)	The address of the CyberArk Server
search	Searches according to the Safe name. Search is performed according to the REST standard (search=search word)
offset	Offset of the first Safe that is returned in the collection of results
limit	The maximum number of Safes that are returned. When used together with the offset parameter, this value determines the number of Safes to return, starting from the first Safe that is returned
sort	Sorts according to the safeName property in ascending order (default) or descending order to control the sort direction
includeAccounts	Whether or not to return accounts for each Safe as part of the response. If not sent, the value is False
extendedDetails	Whether or not to return all Safe details or only safeName as part of the response. If not sent, the value is True.

Outputs	Description
value (value)	The list of Safes
count(count)	
nextLink(nextLink)	

CyberArk/Get Safe Details

This method returns information about a specific Safe in the Vault.



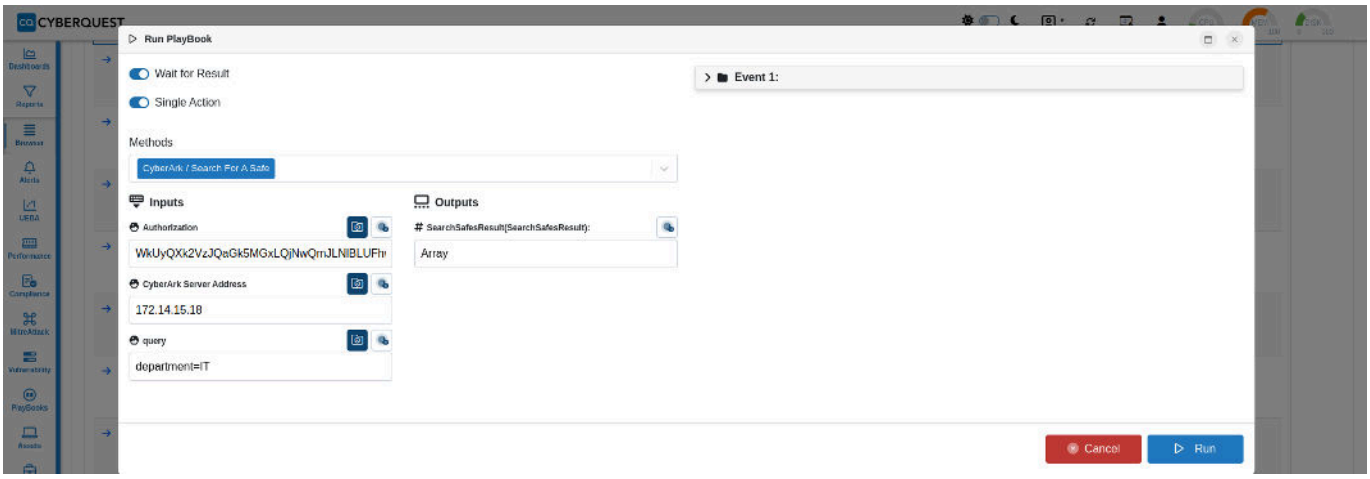


Inputs	Description
Authorization (is required)	The token that identifies the session, encoded in BASE 64
CyberArk Server Address (is required)	The address of the CyberArk Server
SafeUrlId (is required)	The unique ID of the Safe

Outputs	Description
safeUrlId (safeUrlId)	The unique ID of the Safe used when calling Safe APIs
safeName(safeName)	The unique name of the Safe
safeNumber(safeNumber)	The unique numerical ID of the Safe
description(description)	The description of the Safe
location(location)	The location of the Safe in the Vault
creator(creator)	Contains the following parameters: creator.id:The ID of the user that created the Safe. Type: String, creator.name: The name of the user that created the Safe
olacEnabled(olacEnabled)	Whether or not to enable Object Level Access Control for the new Safe
managingCPM(managingCPM)	The name of the CPM user who will manage the new Safe
numberOfVersionsRetention(numberOfVersionsRetention)	The number of retained versions of every password that is stored in the Safe
numberOfDaysRetention(numberOfDaysRetention)	The number of days that password versions are saved in the Safe
autoPurgeEnabled(autoPurgeEnabled)	“Whether or not to automatically purge files after the end of the Object History Retention Period defined in the Safe properties. Report Safes and PSM Recording Safes are created automatically with AutoPurgeEnabled set to Yes. These Safes cannot be managed by the CPM
creationTime(creationTime)	The Unix creation time of the Safe
lastModificationTime(lastModificationTime)	The Unix time when the Safe was last updated
accounts(accounts)	Contains the following parameters: account.id: The ID of the accounts that reside in this Safe, account.name: The name of the accounts that reside in this Safe
isExpiredMember(isExpiredMember)	Whether or not the membership for the Safe is expired. For expired members, the value is True

CyberArk/Search For A Safe

This method returns information about the Safes in the Vault that meet the criteria specified in the search query.

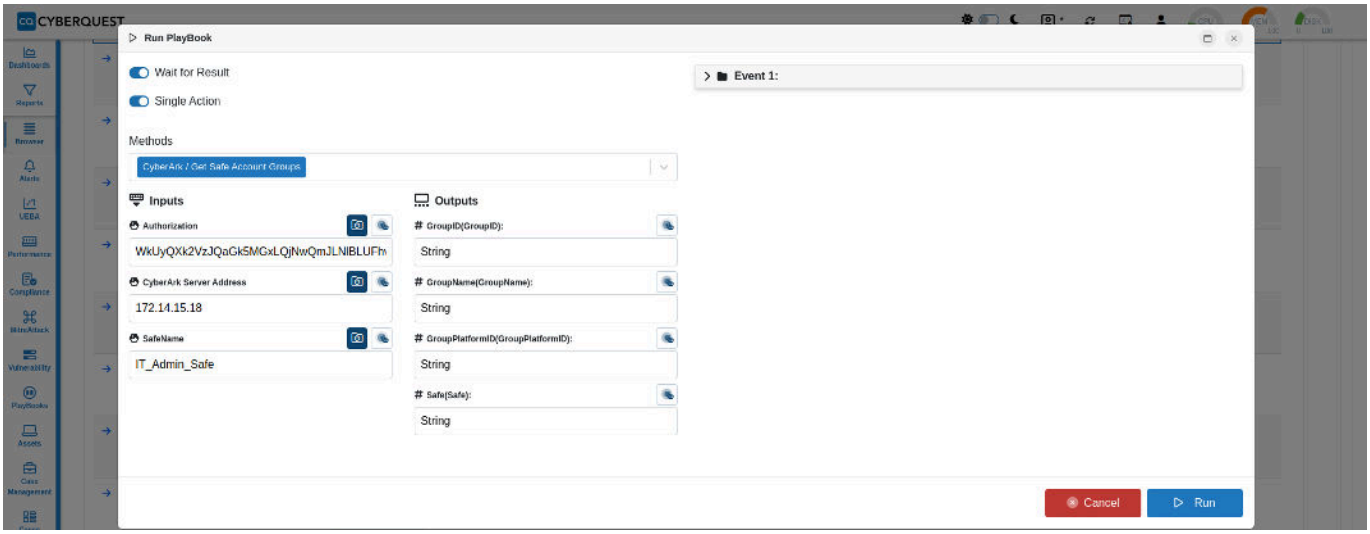


Inputs	Description
Authorization (is required)	The token that identifies the session, encoded in BASE 64
CyberArk Server Address (is required)	The address of the CyberArk Server
query (is required)	The search query

Outputs	Description
SearchSafesResult (SearchSafesResult)	The list of Safes

CyberArk/Get Safe Account Groups

This method returns all the existing account groups in a specific Safe.

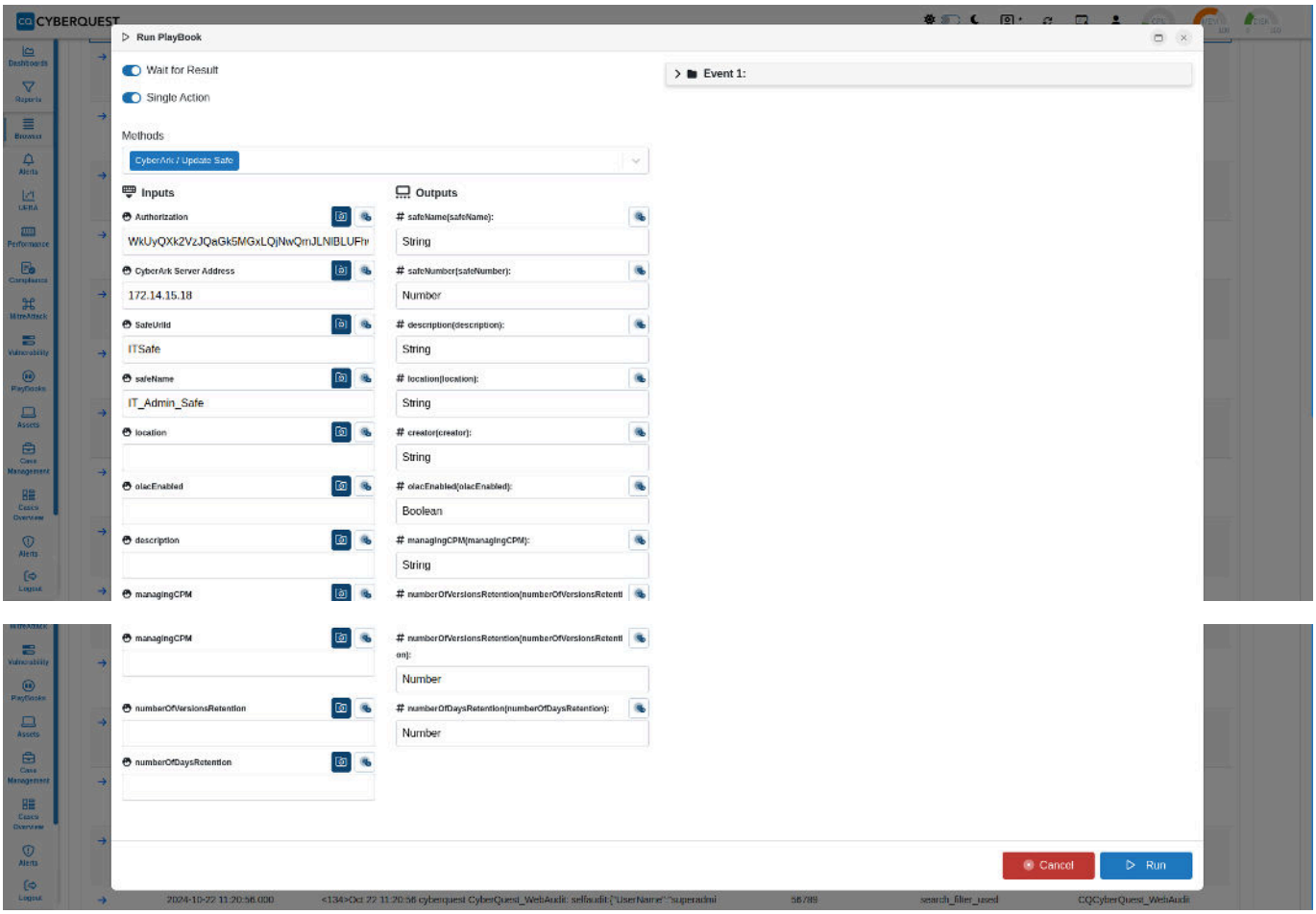


Inputs	Description
Authorization (is required)	The token that identifies the session, encoded in BASE 64
CyberArk Server Address (is required)	The address of the CyberArk Server
SafeName (is required)	The name of the Safe where the account groups are

Outputs	Description
GroupID (GroupID)	The ID of the account group
GroupName(GroupName)	The name of the account group.
GroupPlatformID(GroupPlatformID)	The ID of the platform associated with the account group
Safe(Safe)	The name of the Safe where the account groups are

CyberArk/Update Safe

This method returns all the existing account groups in a specific Safe.

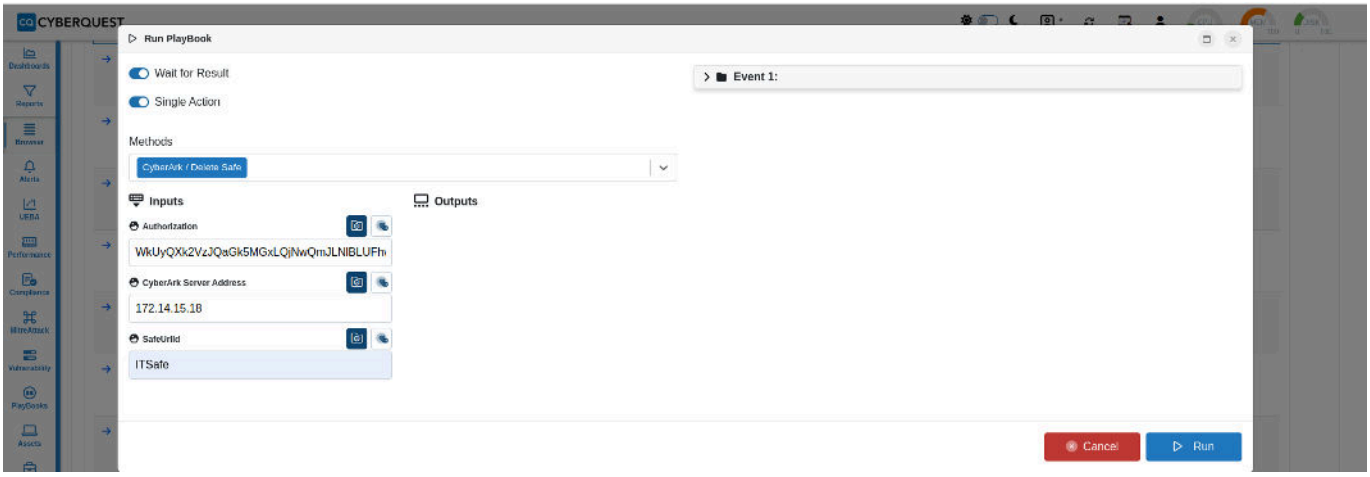


Inputs	Description
Authorization (is required)	The token that identifies the session, encoded in BASE 64
CyberArk Server Address (is required)	The address of the CyberArk Server
SafeUrlId (is required)	The unique ID of the Safe
safeName (is required)	The unique name of the Safe
location	The location of the Safe in the Vault
olacEnabled	Whether to enable Object Level Access Control for the new Safe
description	The description of the Safe
managingCPM	The name of the CPM user who will manage the new Safe
numberOfVersionsRetention	The number of retained versions of every password that is stored in the Safe
numberOfDaysRetention	The number of days that password versions are saved in the Safe

Outputs	Description
safeName (safeName)	The unique name of the Safe
safeNumber(safeNumber)	The unique numerical ID of the Safe
description(description)	The description of the Safe
location(location)	The location of the Safe in the Vault
creator(creator)	Contains the following parameters: creator.id:The ID of the user that created the Safe. Type: String, creator.name: The name of the user that created the Safe
olacEnabled(olacEnabled)	Whether or note to enable Object Level Access Control for the new Safe
managingCPM(managingCPM)	The name of the CPM user who will manage the new Safe
numberOfVersionsRetention(numberOfVersionsRetention)	The number of retained versions of every password that is stored in the Safe
numberOfDaysRetention(numberOfDaysRetention)	The number of days that password versions are saved in the Safe

CyberArk/Delete Safe

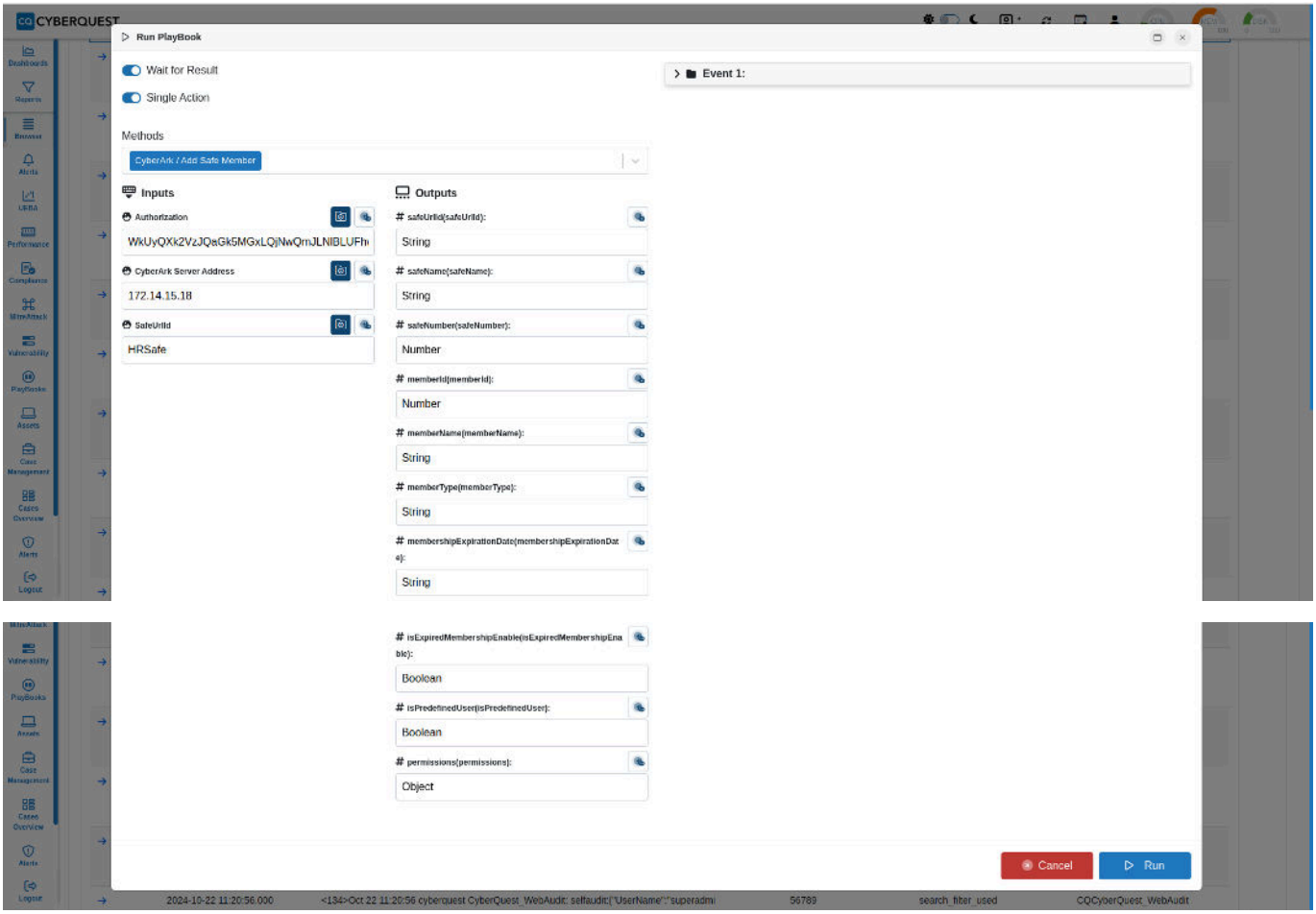
This method deletes a Safe from the Vault.



Inputs	Description
Authorization (is required)	The token that identifies the session, encoded in BASE 64
CyberArk Server Address (is required)	The address of the CyberArk Server
SafeUrlId (is required)	The unique ID of the Safe

CyberArk/Add Safe Member

This method adds an existing user or group as a Safe member.

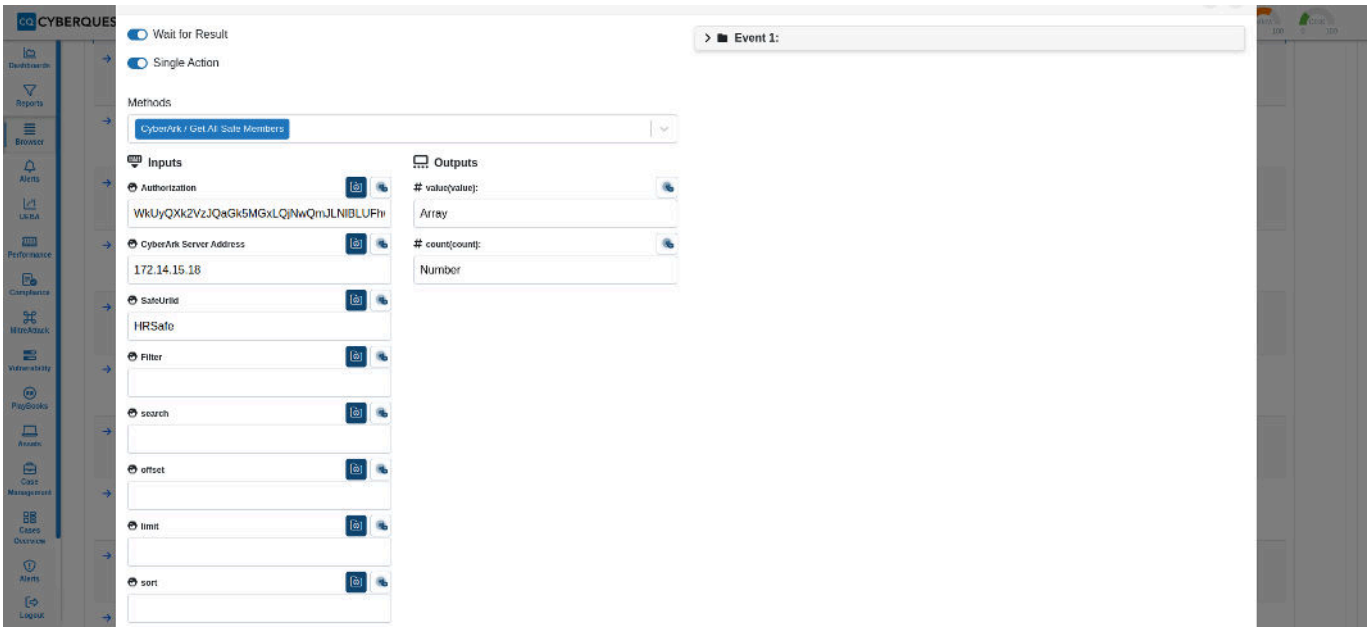


Inputs	Description
Authorization (is required)	The token that identifies the session, encoded in BASE 64
CyberArk Server Address (is required)	The address of the CyberArk Server
SafeUrlId (is required)	The unique ID of the Safe

Outputs	Description
safeUrlId (safeUrlId)	The unique ID of the Safe used when calling Safe APIs
safeName(safeName)	The unique name of the Safe
safeNumber(safeNumber)	The unique numerical ID of the Safe
memberId(memberId)	The Vault user ID, Domain user ID, or group ID of the Safe member
memberName(memberName)	The Vault user name, Domain user name or group name of the Safe member
memberType(memberType)	The member type
membershipExpirationDate(membershipExpirationDate)	The members expiration date for this Safe. For members that do not have an expiration date, this value will be null
isExpiredMembershipEnable(isExpiredMembershipEnable)	Whether or not the membership for the Safe is expired. For expired members, the value is True
isPredefinedUser(isPredefinedUser)	Whether the member is a predefined Vault user or group
permissions(permissions)	The permissions that the user or group has on this

CyberArkGet/All Safe Members

This method returns a list of the members of a Safe.

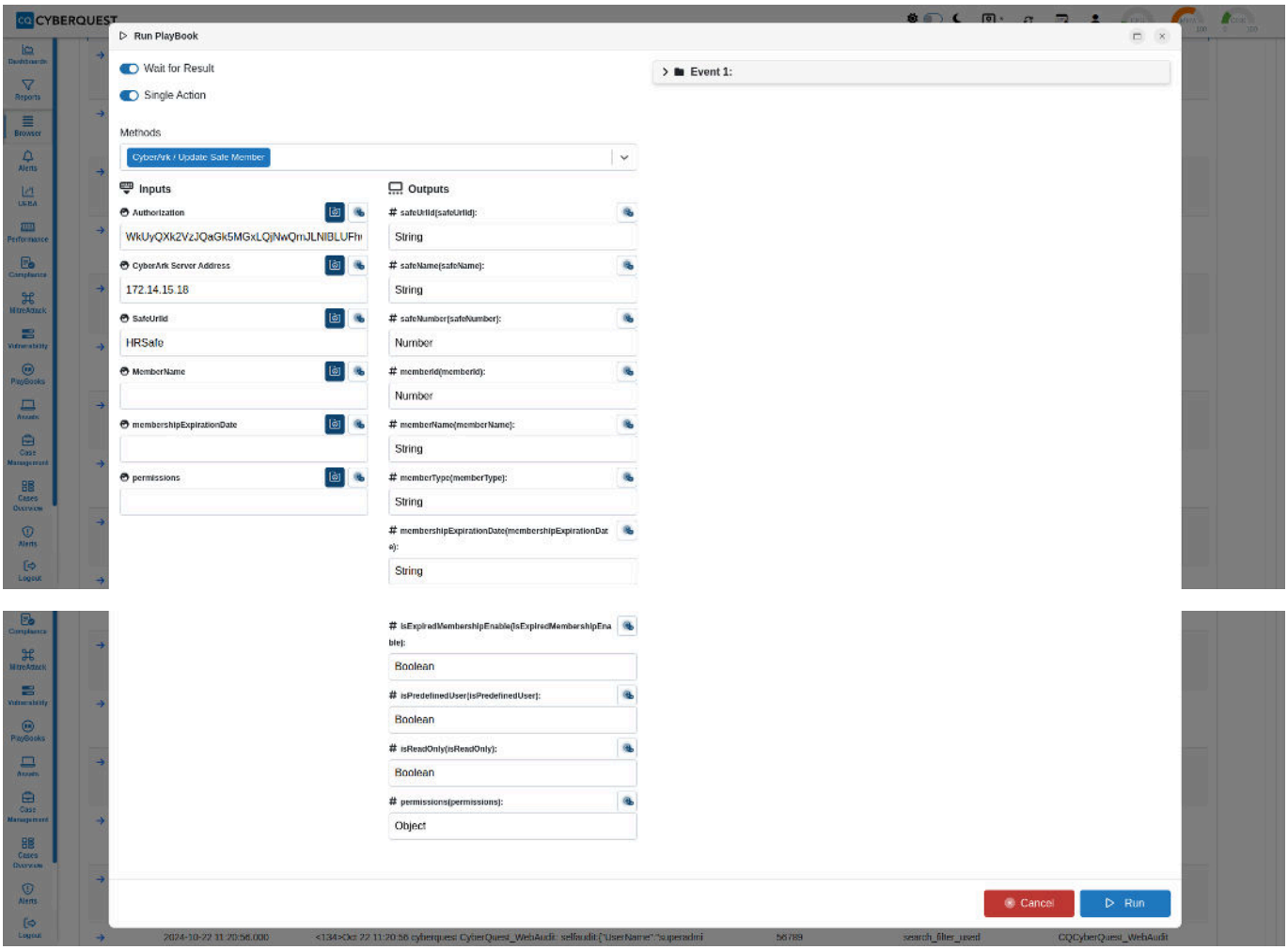


Inputs	Description
Authorization (is required)	The token that identifies the session, encoded in BASE 64
CyberArk Server Address (is required)	The address of the CyberArk Server
SafeUrlId (is required)	The unique ID of the Safe
Filter	Filters are according to the REST standard. Search for Safe members using the following filters. Multiple filters can be applied using the AND operator
search	Searches according to the Safe name. Search is performed according to the REST standard (search=search word)
offset	Offset of the first member that is returned in the collection of results
limit	The maximum number of members that are returned
sort	Sorts according to the memberName property in ascending order (default) or descending order to control the sort direction

Outputs	Description
value (value)	The list of all safe members
count(count)	The number of members

CyberArkGet/Update Safe Member

This method updates an existing Safe member.

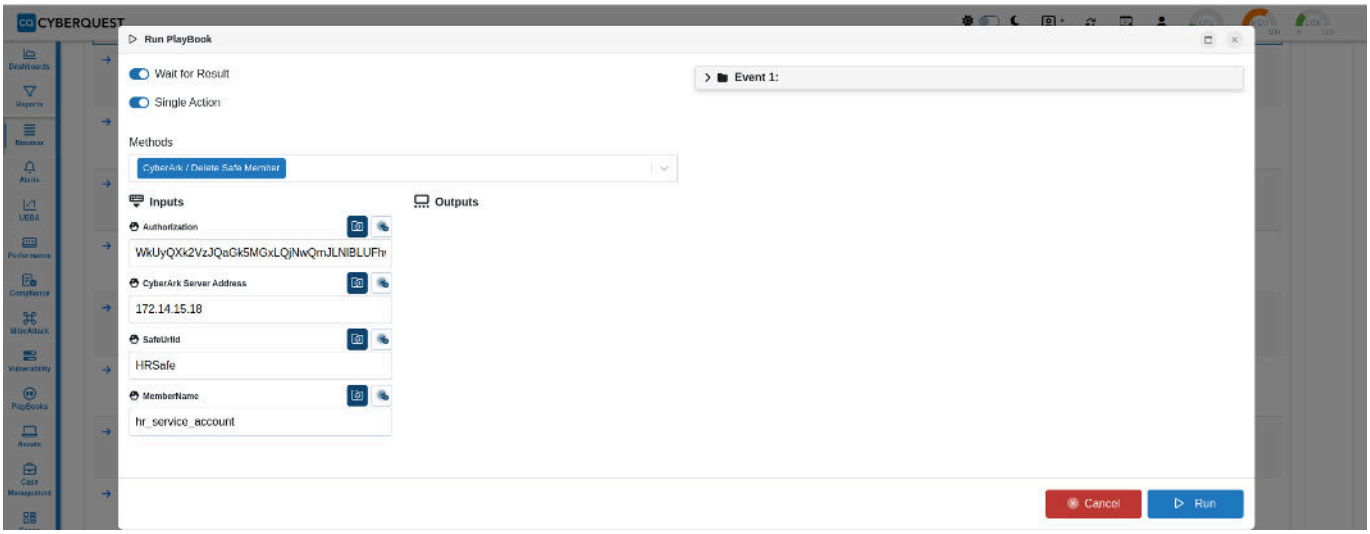


Inputs	Description
Authorization (is required)	The token that identifies the session, encoded in BASE 64
CyberArk Server Address (is required)	The address of the CyberArk Server
SafeUrlId (is required)	The unique ID of the Safe
MemberName	The Vault user name, Domain user name or group name of the Safe member
membershipExpirationDate	The Vault user name, Domain user name or group name of the Safe member
permissions	User or group permissions in the Safe

Outputs	Description
safeUrlId (safeUrlId)	The unique ID of the Safe used when calling Safe APIs
safeName(safeName)	The unique name of the Safe
safeNumber(safeNumber)	The unique numerical ID of the Safe
memberId(memberId)	The Vault user ID, Domain user ID, or group ID of the Safe member
memberName(memberName)	The Vault user name, Domain user name or group name of the Safe member
memberType(memberType)	The member type
membershipExpirationDate(membershipExpirationDate)	The members expiration date for this Safe. For members that do not have an expiration date, this value will be null
isExpiredMembershipEnable(isExpiredMembershipEnable)	Whether or not the membership for the Safe is expired. For expired members, the value will be True
isPredefinedUser(isPredefinedUser)	Whether the member is a predefined user or group of the Vault
isReadOnly(isReadOnly)	Whether or not the current user can update the permissions of a member
permissions	The permissions that the user or group has for this Safe

CyberArkGet/Delete Safe Member

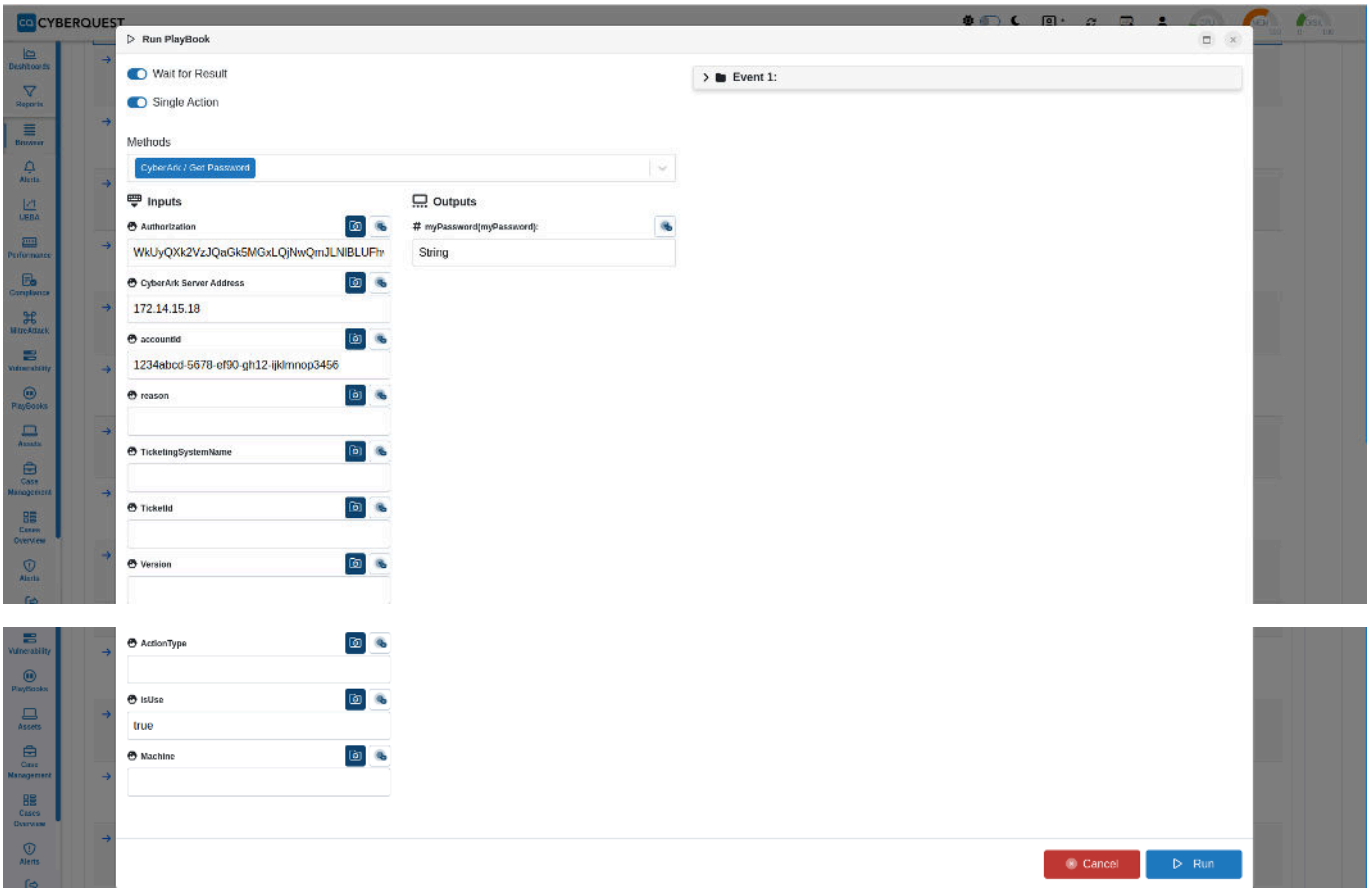
This method removes a specific member from a Safe.



Inputs	Description
Authorization (is required)	The token that identifies the session, encoded in BASE 64
CyberArk Server Address (is required)	The address of the CyberArk Server
SafeUrlId (is required)	The unique ID of the Safe
MemberName (is required)	The Vault user name, Domain user name or group name of the Safe member

CyberArkGet/Get Password

This method enables users to retrieve the password or SSH key of an existing account that is identified by its Account ID. It enables users to specify a reason and ticket ID, if required.



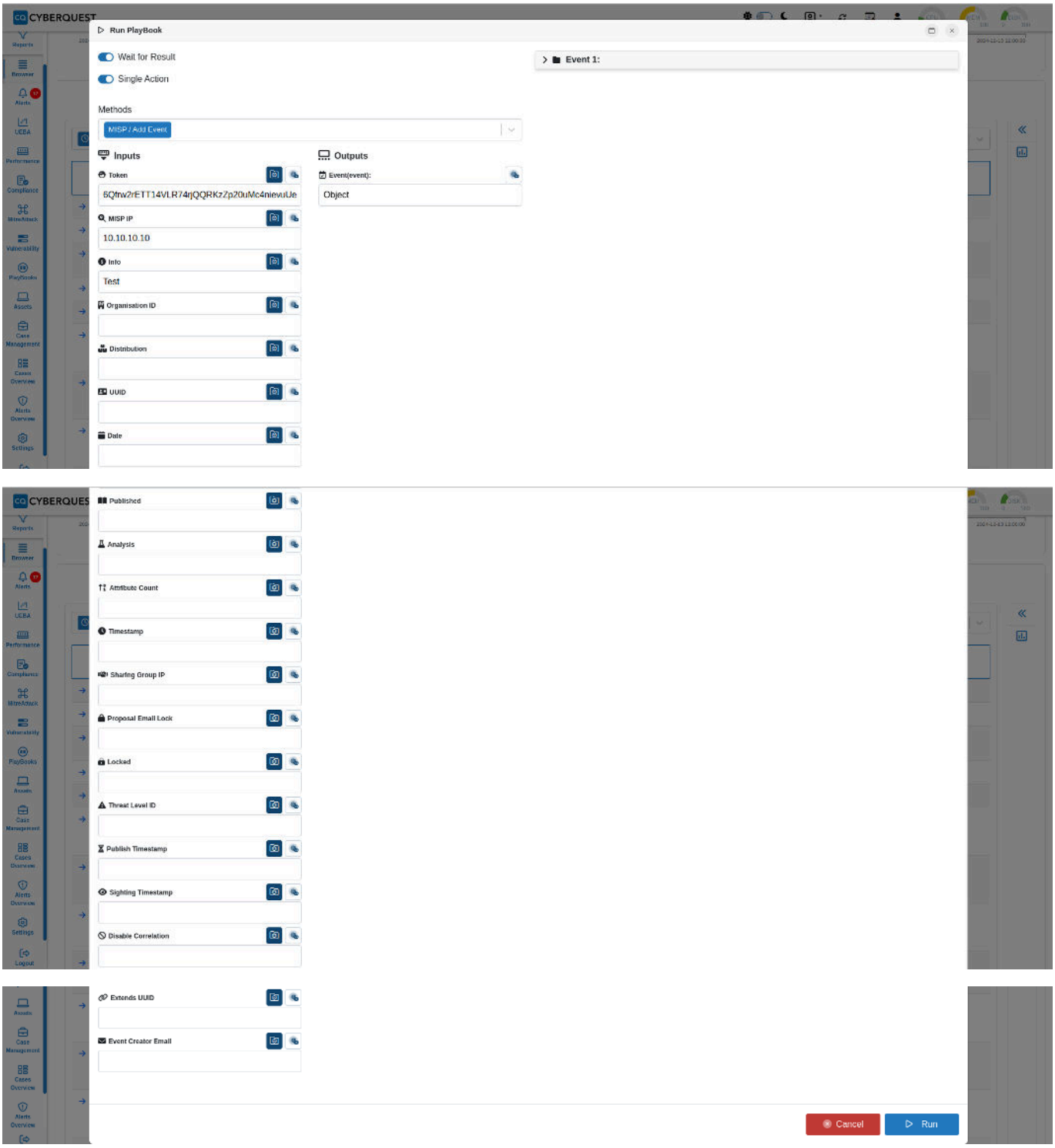
Inputs	Description
Authorization (is required)	The token that identifies the session, encoded in BASE 64
CyberArk Server Address (is required)	The address of the CyberArk Server
accountId (is required)	The unique ID of the account
reason	The reason that is required to retrieve the password/SSH key
TicketingSystemName	The name of the Ticketing System
TicketId	The Vault user name, Domain user name or group name of the Safe member
Version	The Vault user name, Domain user name or group name of the Safe member
ActionType	The action this password will be used for
isUse (is required)	Internal parameter (for PSM for SSH only)
Machine	The address of the remote machine to connect to

Outputs	Description
myPassword (myPassword)	The password of the account

MISP

MISP/Add Event

Enables the creation and management of events related to cybersecurity intelligence.

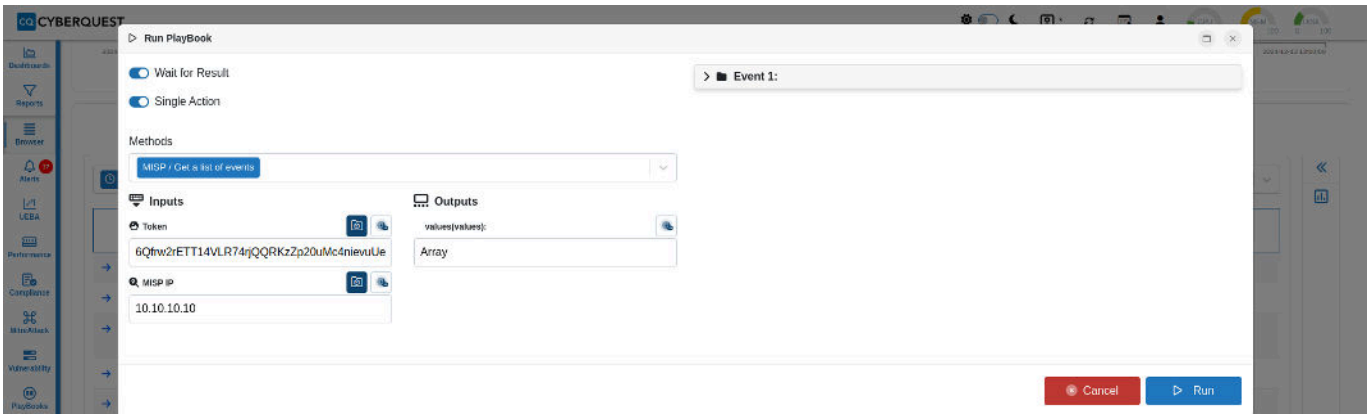

CYBERQUEST
Run PlayBook
Wait for Result
Single Action
Methods
MISP / Add Event
Inputs
Token
6Qfnv2rETT14VLR74rjQQRKzZp20uMc4nievuUe
MISP IP
10.10.10.10
Info
Test
Organisation ID
Distribution
UUID
Date
Outputs
Event(event):
Object
Event 1:
Published
Analysis
Attribute Count
Timestamp
Sharing Group ID
Proposal Email Lock
Locked
Threat Level ID
Publish Timestamp
Sighting Timestamp
Disable Correlation
Extends UUID
Event Creator Email
Cancel
Run

Inputs	Description
Token (is required)	To use the MISP API, you must have an API key
MISP IP (is required)	The IP of the MISP serverThe IP of the MISP server
Info (is required)	Details about the event
Organisation ID	It refers to the unique identifier for an organization within the MISP platform
Distribution	Who will be able to see this event once it becomes published and eventually when it becomes pulled: 0 Your organization only 1 This community only 2 Connected communities 3 All communities 4 Sharing group 5 Inherit Event
UUID	It is a universally unique identifier used to uniquely identify and manage events, attributes, or other objects within the platform. It ensures that each entity is distinct and easily traceable across MISP
Date	Represents the timestamp or specific date associated with an event
Published	Indicates whether an event or attribute is publicly shared or not
Analysis	Represents the analysis maturity level. 0: Initial 1: Ongoing 2: Complete
Attribute Count	The number of the attributes from the event
Timestamp	The exact date and time when an event, attribute, or other data is created or updated
Sharing Group IP	Is used to associate an event or attribute with a specific sharing group
Proposal Email Lock	Is used to control whether a proposal (event or attribute) can be modified or edited by others after being submitted via email
Locked	Indicates whether an event or attribute is locked, preventing further modifications.
Threat Level ID	Represents the threat level. 1: High 2: Medium 3: Low 4: Undefined
Publish Timestamp	Represents the date and time when an event or attribute is published, indicating its visibility and availability for sharing with external systems or organizations
Sighting Timestamp	Records the date and time when a specific observation or sighting of a cyber threat was made.
Disable Correlation	Allows users to prevent the correlation of certain attributes or events with other data.
Extends UUID	Is used to link an attribute or event to another existing event or attribute using its unique UUID.
Event Creator Email	Stores the email address of the user who created the event. It helps in tracking the origin and ownership of specific cybersecurity events

Outputs	Description
Event (event)	The informations with which the event was created

MISP/Get a list of events

Retrieves a list of events based on specified filters, enabling efficient access to relevant threat intelligence data.

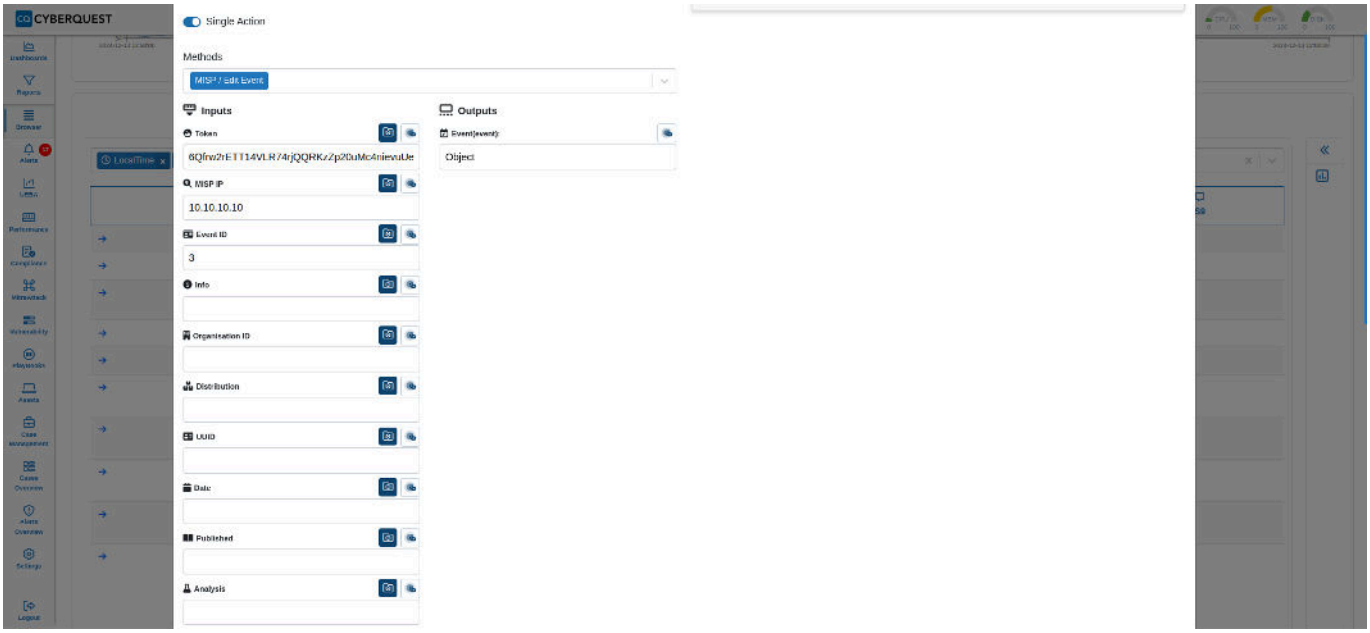


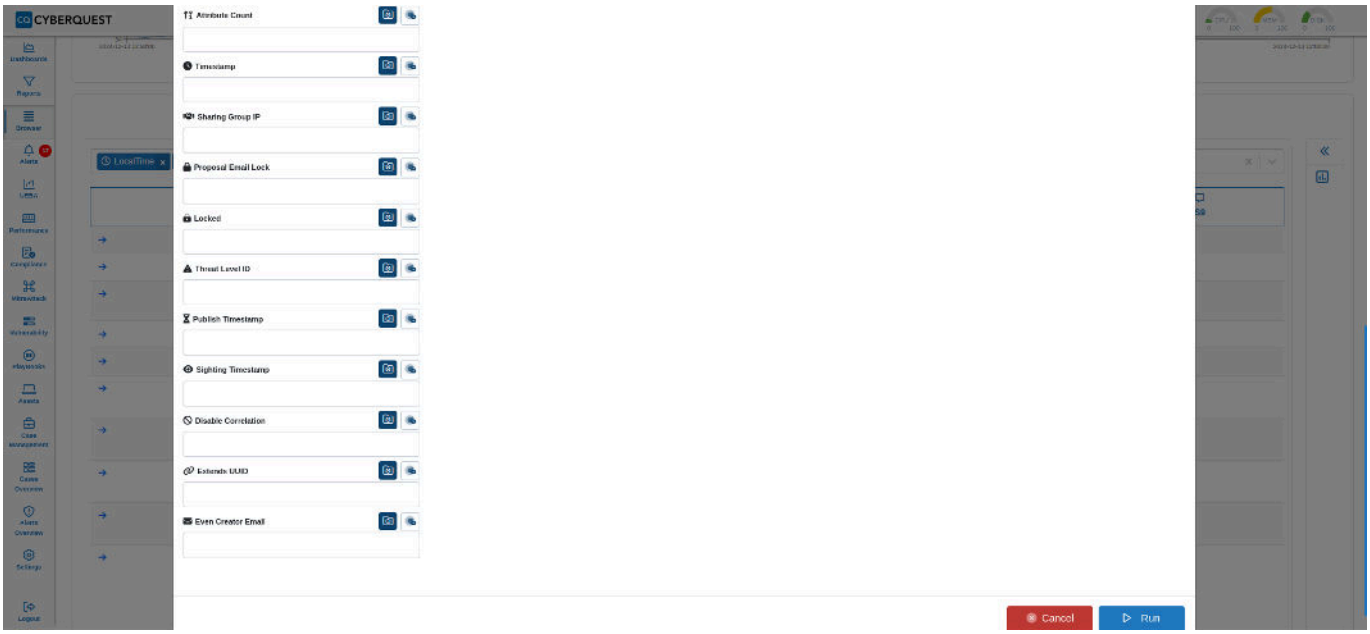
Inputs	Description
Token (is required)	To use the MISP API, you must have an API key
MISP IP (is required)	The IP of the MISP server

Outputs	Description
values (values)	The results of the API call

MISP/Edit Event

Allows modifications to an existing event.



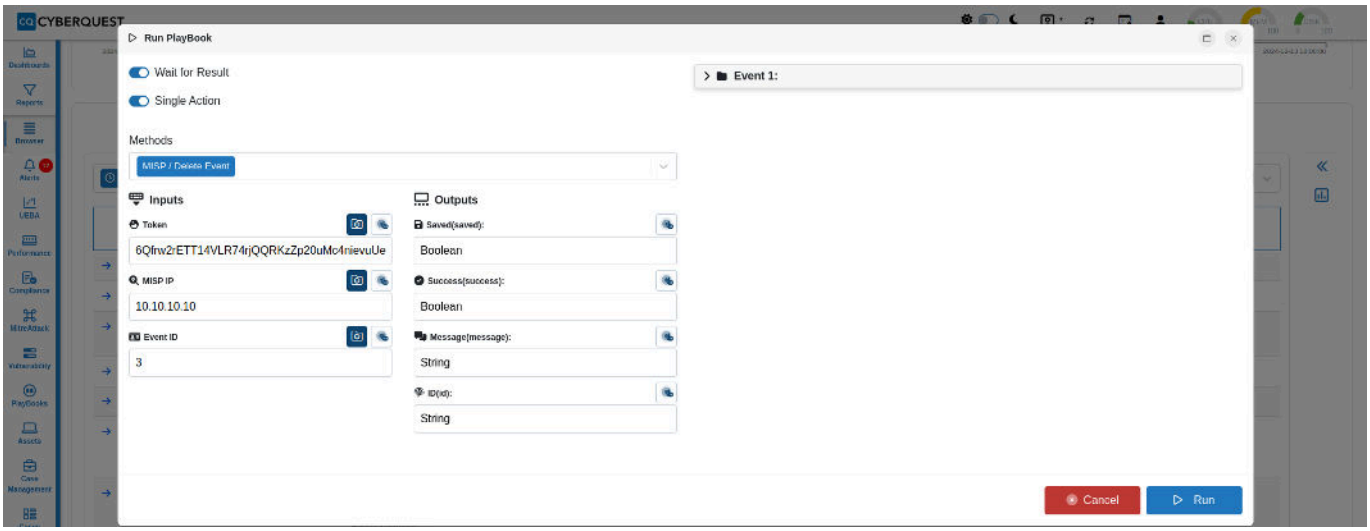

CYBERQUEST
Attribute Count
Timestamp
Sharing Group ID
Proposal Email Lock
Locked
Threat Level ID
Publish Timestamp
Sighting Timestamp
Disable Correlation
Extends UUID
Even Creator Email
Cancel
Run

Inputs	Description
Token (is required)	To use the MISP API, you must have an API key
MISP IP (is required)	The IP of the MISP server
Event ID (is required)	The ID of the event which is wanted to be edited
Info	Details about the event
Organisation ID	It refers to the unique identifier for an organization within the MISP platform
Distribution	Who will be able to see this event once it becomes published and eventually when it becomes pulled: 0 Your organization only 1 This community only 2 Connected communities 3 All communities 4 Sharing group 5 Inherit Event
UUID	It is a universally unique identifier used to uniquely identify and manage events, attributes, or other objects within the platform. It ensures that each entity is distinct and easily traceable across MISP
Date	Represents the timestamp or specific date associated with an event
Published	Indicates whether an event or attribute is publicly shared or not
Analysis	Represents the analysis maturity level. 0: Initial 1: Ongoing 2: Complete
Attribute Count	The number of the attributes from the event
Timestamp	The exact date and time when an event, attribute, or other data is created or updated
Sharing Group IP	Is used to associate an event or attribute with a specific sharing group
Proposal Email Lock	Is used to control whether a proposal (event or attribute) can be modified or edited by others after being submitted via email
Locked	Indicates whether an event or attribute is locked, preventing further modifications.
Threat Level ID	Represents the threat level. 1: High 2: Medium 3: Low 4: Undefined
Publish Timestamp	Represents the date and time when an event or attribute is published, indicating its visibility and availability for sharing with external systems or organizations
Sighting Timestamp	Records the date and time when a specific observation or sighting of a cyber threat was made.
Disable Correlation	Allows users to prevent the correlation of certain attributes or events with other data.
Extends UUID	Is used to link an attribute or event to another existing event or attribute using its unique UUID.
Even Creator Email	Stores the email address of the user who created the event. It helps in tracking the origin and ownership of specific cybersecurity events

Outputs	Description
Event (event)	The informations with which the event was edited

MISP/Delete Event

Removes an existing event and its associated data from the platform.

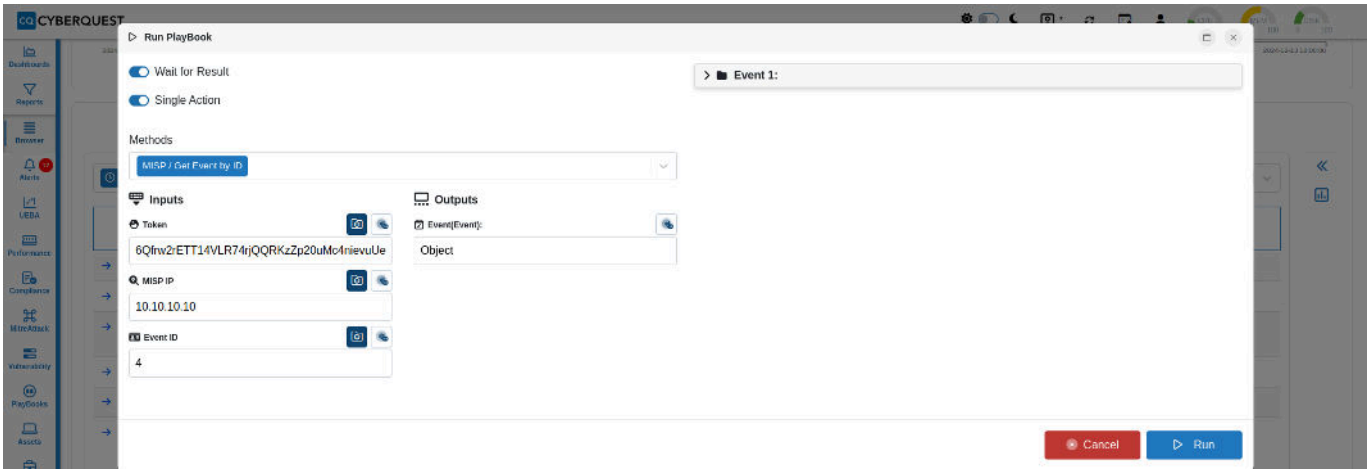


Inputs	Description
Token (is required)	To use the MISP API, you must have an API key
MISP IP (is required)	The IP of the MISP server
Event ID (is required)	The ID of the event which is wanted to be deleted

Outputs	Description
Saved (saved)	True if the operation was successful, otherwise False
Success (success)	True if the operation was successful, otherwise False
Message (message)	The message about the action which was realised
ID (id)	The ID of the event on which action was realized

MISP/Get Event by ID

Retrieves detailed information about a specific event using its unique identifier.

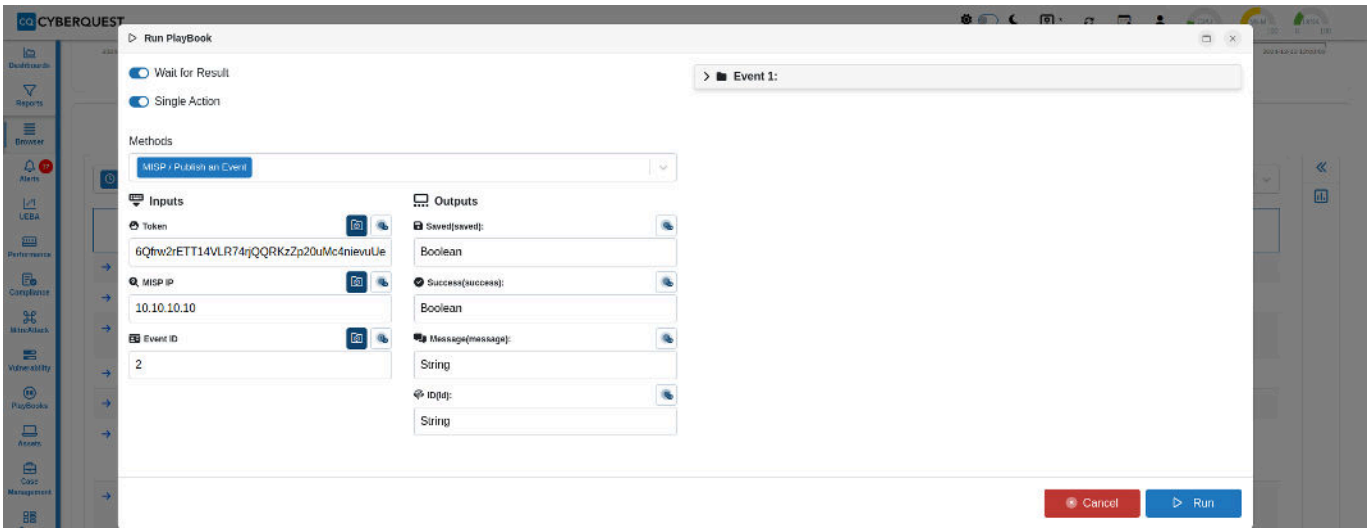


Inputs	Description
Token (is required)	To use the MISP API, you must have an API key
MISP IP (is required)	The IP of the MISP server
Event ID (is required)	The ID of the event which is wanted to be searched

Outputs	Description
Event (Event)	The informations of the searched event

MISP/Publish an Event

Allows users to publish an event, making it available for sharing with other MISP instances or organizations while maintaining control over visibility.

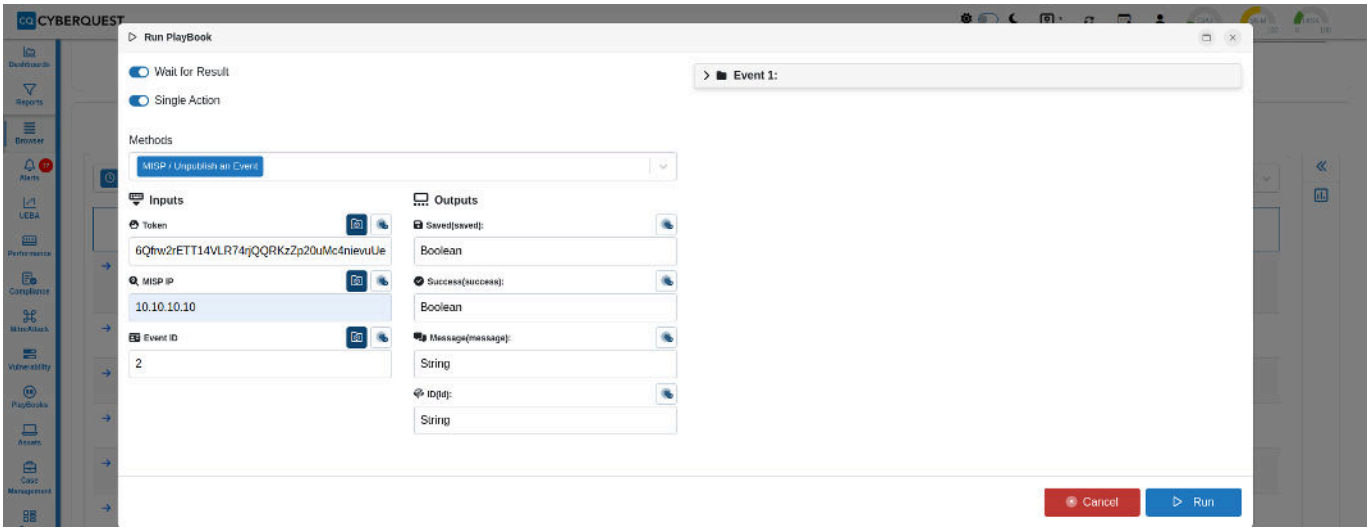


Inputs	Description
Token (is required)	To use the MISP API, you must have an API key
MISP IP (is required)	The IP of the MISP server
Event ID (is required)	The ID of the event which is wanted to be published

Outputs	Description
Saved (saved)	True if the operation was successful, otherwise False
Success (success)	True if the operation was successful, otherwise False
Message (message)	The message about the action which was realised
ID (id)	The ID of the event on which action was realized

MISP/Unpublish an Event

Allows users to retract the published status of an event, ensuring that it is no longer shared with external parties while keeping it accessible within the MISP instance.

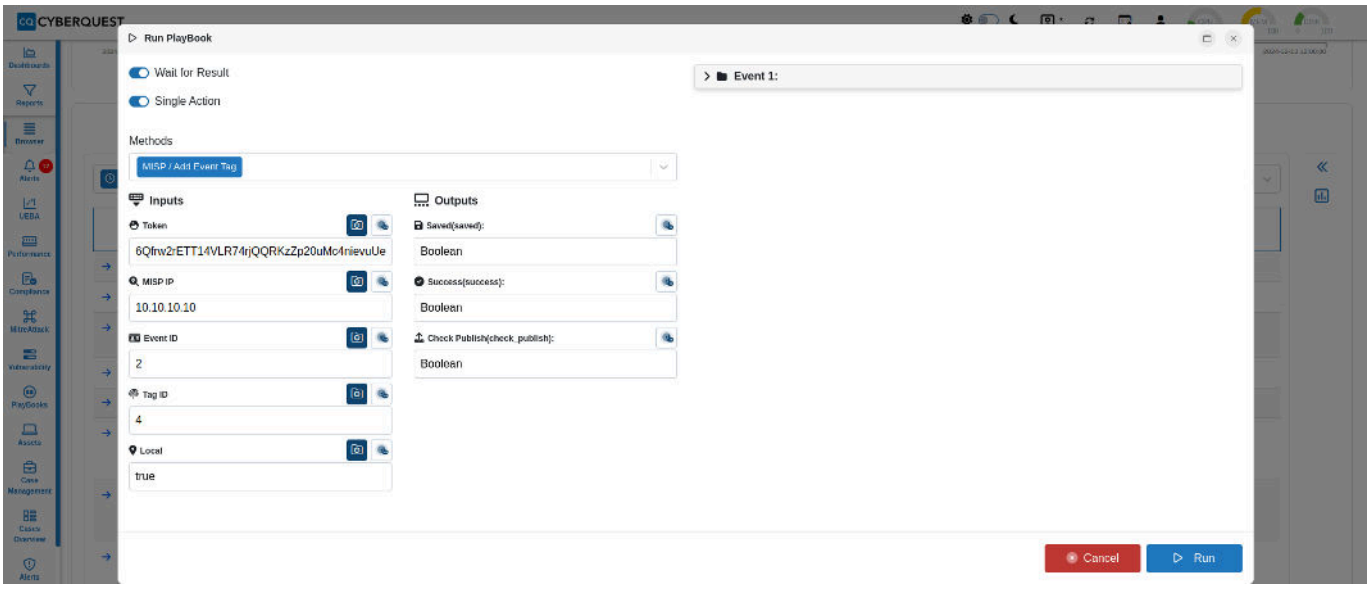


Inputs	Description
Token (is required)	To use the MISP API, you must have an API key
MISP IP (is required)	The IP of the MISP server
Event ID (is required)	The ID of the event which is wanted to be unpublished

Outputs	Description
Saved (saved)	True if the operation was successful, otherwise False
Success (success)	True if the operation was successful, otherwise False
Message (message)	The message about the action which was realised
ID (id)	The ID of the event on which action was realized

MISP/Add Event Tag

Allows users to assign tags to an event for better organization, categorization, and easy identification within the platform.

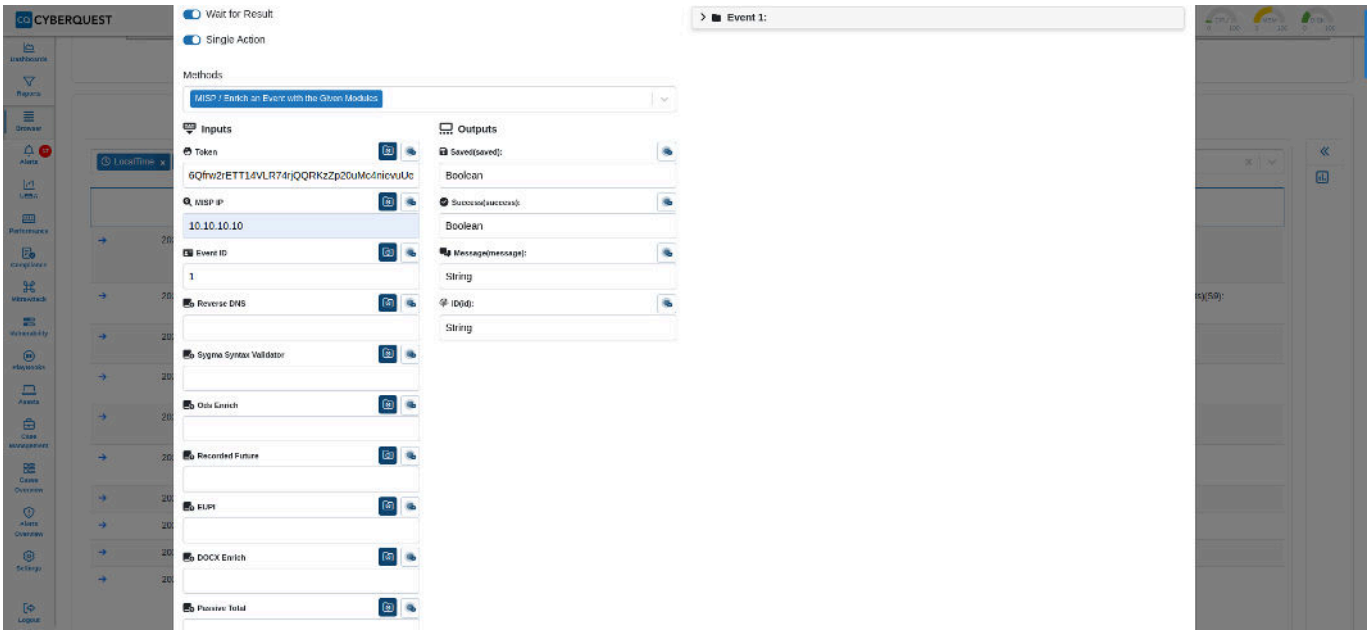


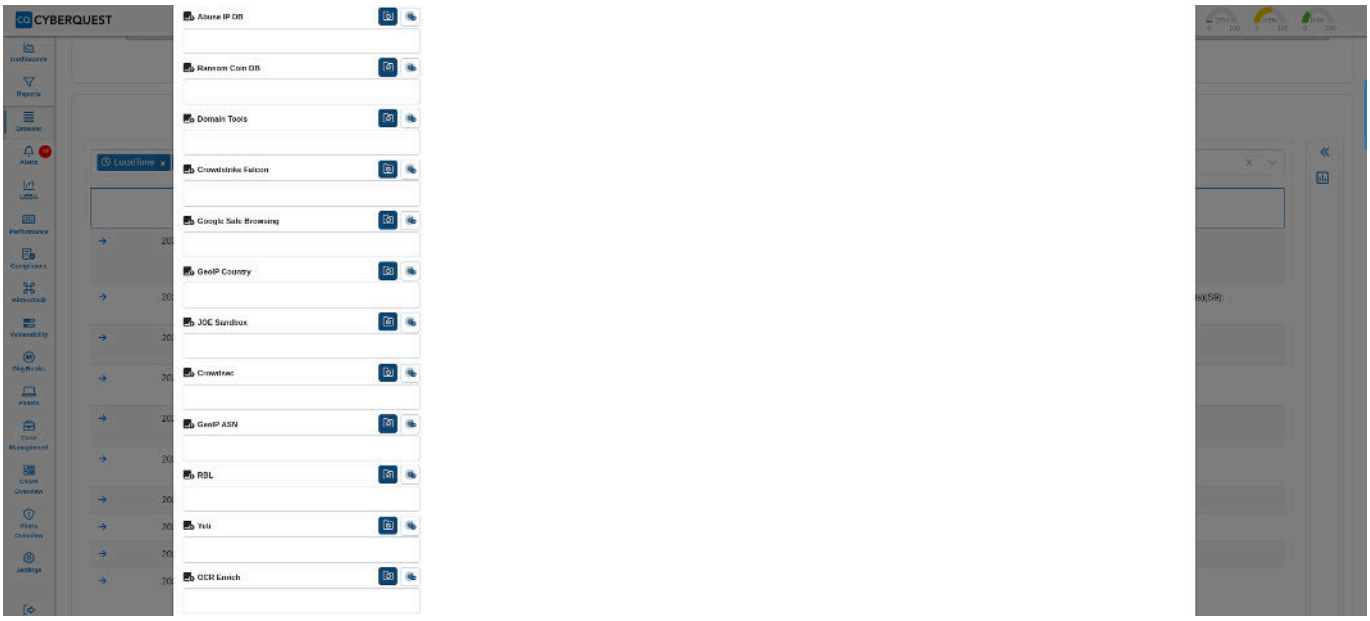
Inputs	Description
Token (is required)	To use the MISP API, you must have an API key
MISP IP (is required)	The IP of the MISP server
Event ID (is required)	The ID of the event where the tag will be added
Tag ID (is required)	Numeric ID of the attribute
Local (is required)	Whether the object should be attached locally or not to the target

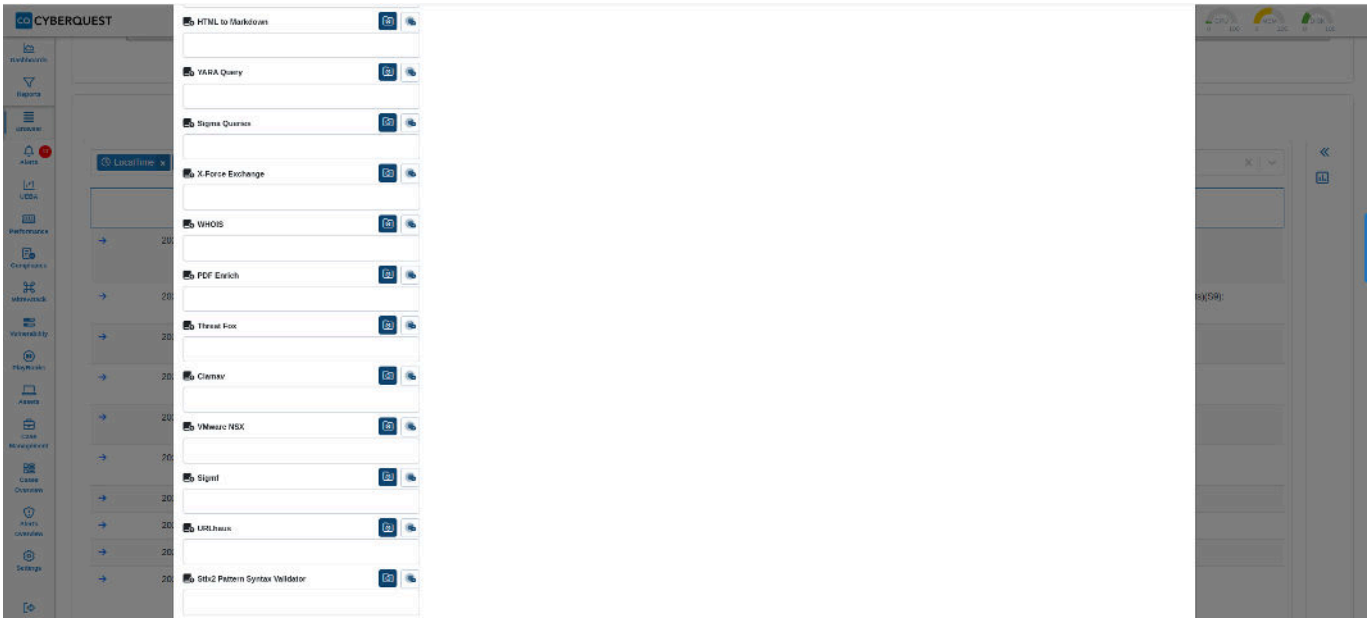
Outputs	Description
Saved (saved)	True if the operation was successful, otherwise False
Success (success)	True if the operation was successful, otherwise False
Check Publish (check_publish)	Is used to verify whether an event or attribute is ready for publication or sharing.

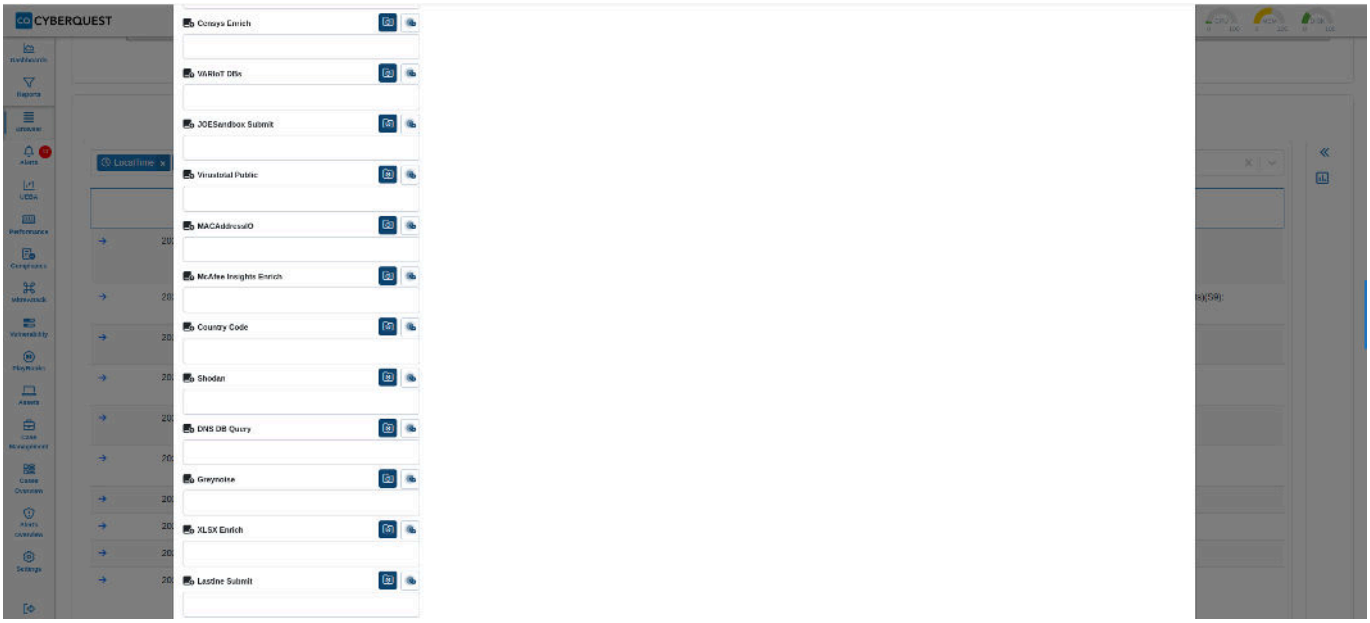
MISP/Enrich an Event with the Given Modules

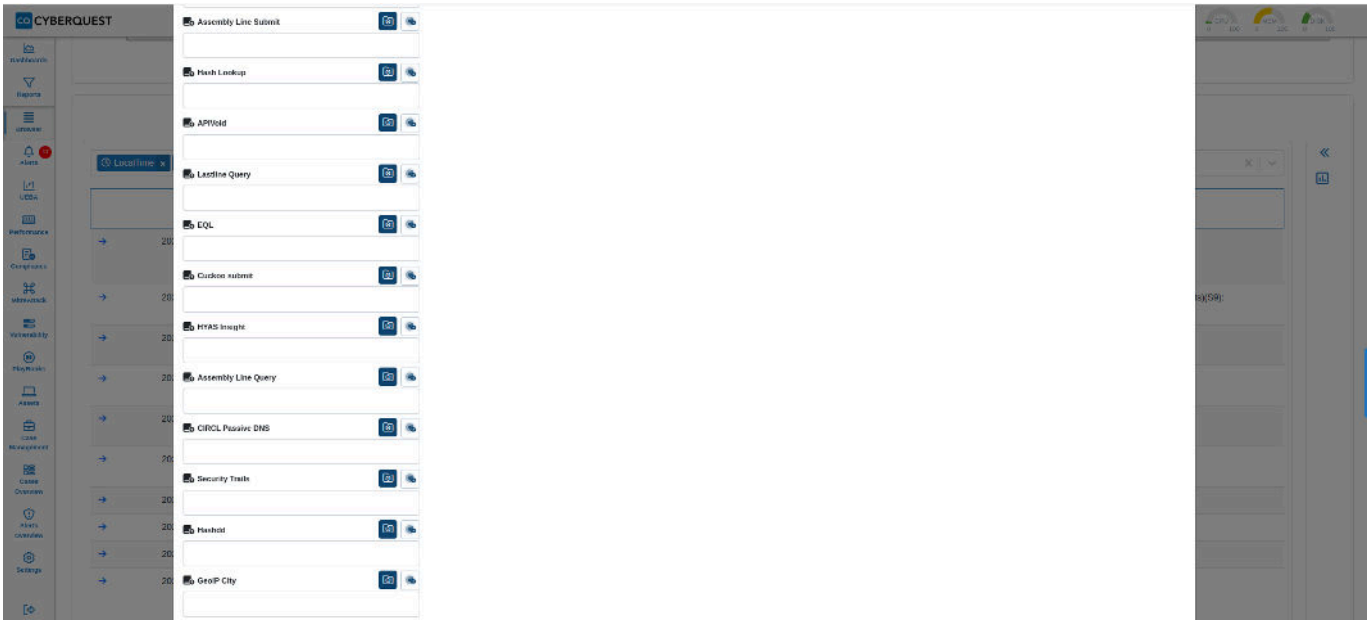
Alows users to enhance an event by applying specific modules, such as automated threat intelligence or data enrichment, to add additional context and insights.

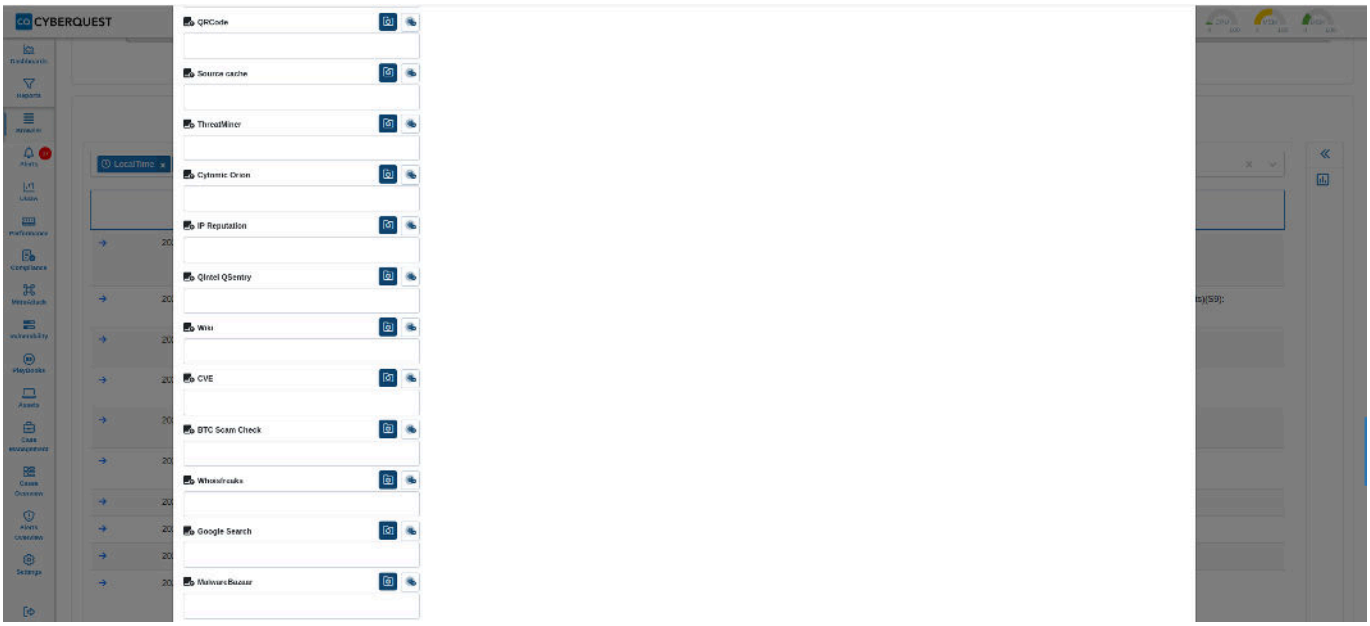

CYBERQUEST
Wait for Result
Single Action
Methods
MISP : Enrich an Event with the Given Modules
Inputs
Token
6Qfrw2rETT14VLR74rjQQRKzZp20uMc4nicvuUc
MISP IP
10.10.10.10
Event ID
1
Reverse DNS
Sygma Syntax Validator
Otx Enrich
Recorded Future
RUPI
DOCX Enrich
Passive Total
Outputs
Saved(saved):
Boolean
Success(success):
Boolean
Message(message):
String
ID(id):
String
Event 1:

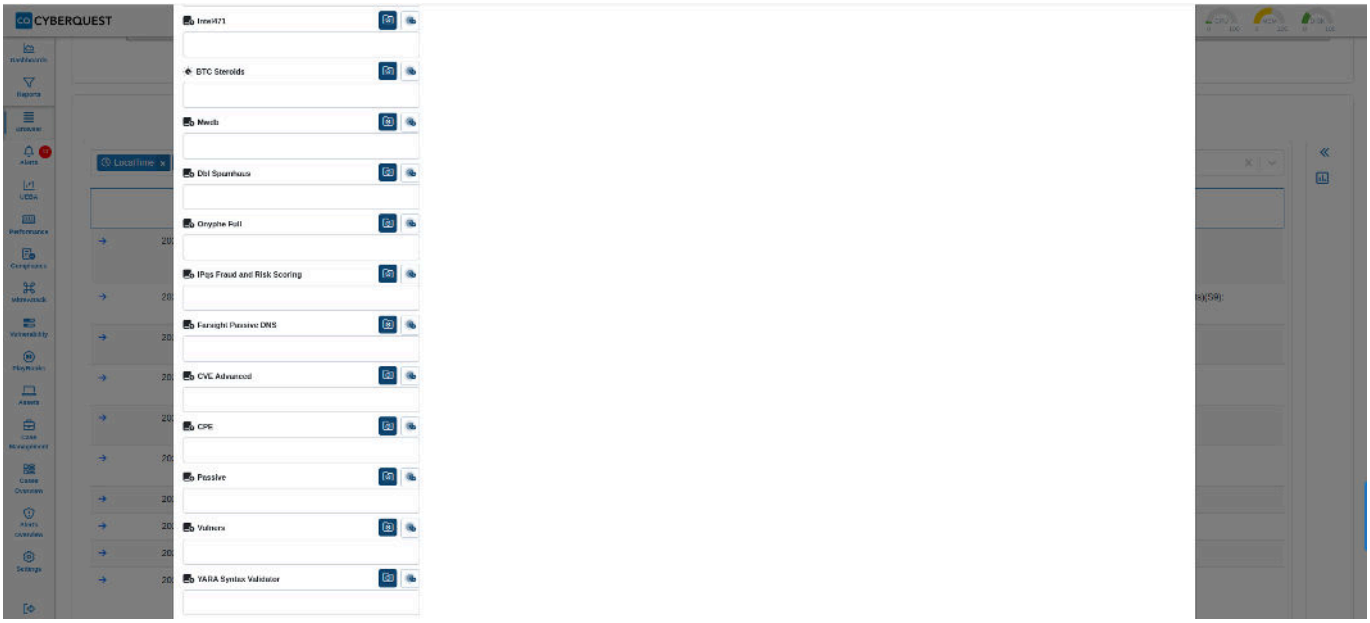

CYBERQUEST
Abuse IP DB
Ransom Coin DB
Domain Tools
Crowdstrike Falcon
Google Safe Browsing
GeoIP Country
JOE Sandbox
Crowdsec
GeoIP ASN
RBL
Yeti
OCR Enrich

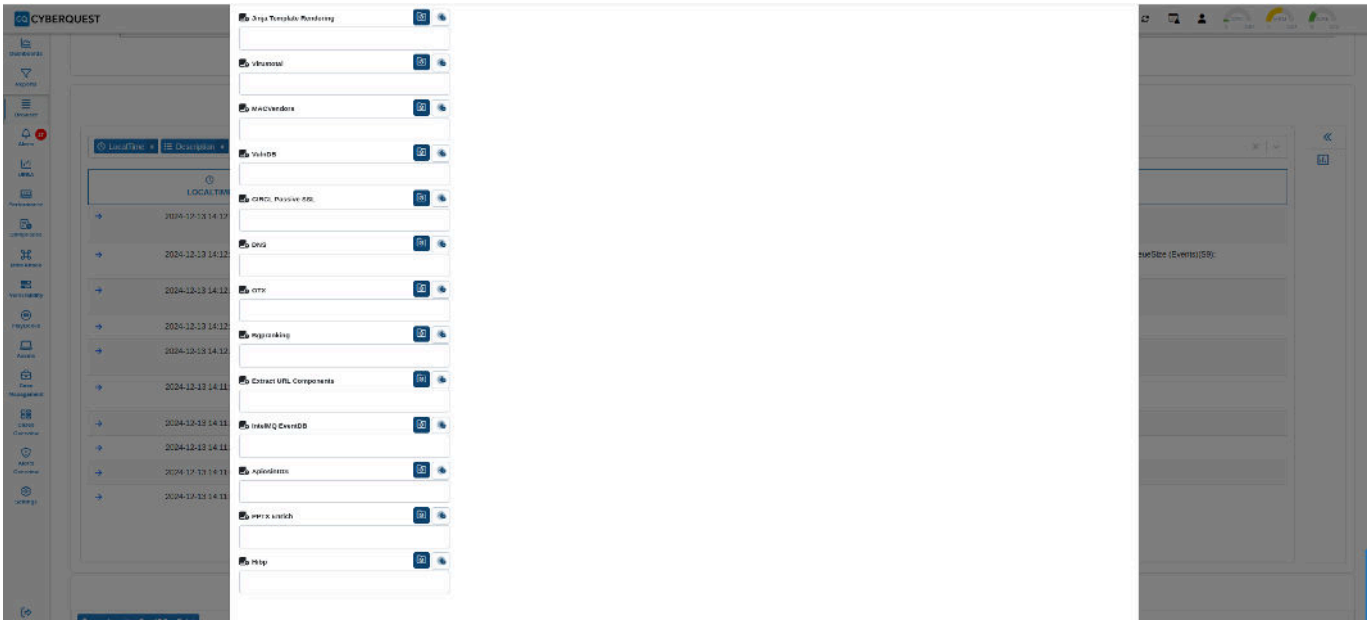

CYBERQUEST
HTML to Markdown
YARA Query
Sigma Queries
X-Force Exchange
WHOIS
PDF Enrich
Threat Fox
Clamav
VMware NSX
Sigml
URLhaus
Stix2 Pattern Syntax Validator


CYBERQUEST
Convex Enrich
VARIoT DBs
JOESandbox Submit
Virustotal Public
MACAddressIO
McAfee Insights Enrich
Country Code
Shodan
DNS DB Query
Greynoise
XLSX Enrich
Lastline Submit


CYBERQUEST
Assembly Line Submit
Hash Lookup
APIVoid
Lastline Query
EQL
Cuckoo submit
HYAS Insight
Assembly Line Query
CIRCL Passive DNS
Security Trails
Hashdd
GeoIP City


CYBERQUEST
QRCode
Source cache
ThreatMiner
Cylomic Orion
IP Reputation
Qintel QSentry
Wiki
CVE
BTC Scam Check
Whoisfreaks
Google Search
MalwareBazaar


CYBERQUEST
Intel471
BTC Steroids
Mwob
Dbl Spamhaus
Onyphe Full
IPqs Fraud and Risk Scoring
Farsight Passive DNS
CVE Advanced
CPE
Passive
Vulners
YARA Syntax Validator


CYBERQUEST
Virustotal
MACVendors
VulnDB
DNS
OTX
Phishtank
Extract URL Components
AbuseIPDB

Inputs	Description
Token (is required)	To use the MISP API, you must have an API key
MISP IP (is required)	The IP of the MISP server
Event ID (is required)	The ID of the event which is wanted to be enhanced
Reverse DNS	The additional module which is used to enrich the event
Sygma Syntax Validator	The additional module which is used to enrich the event
Ods Enrich	The additional module which is used to enrich the event
Recorded Future	The additional module which is used to enrich the event
EUPI	The additional module which is used to enrich the event
DOCX Enrich	The additional module which is used to enrich the event
Passive Total	The additional module which is used to enrich the event
Abuse IP DB	The additional module which is used to enrich the event
Ransom Coin DB	The additional module which is used to enrich the event
Domain Tools	The additional module which is used to enrich the event
Crowdstrike Falcon	The additional module which is used to enrich the event
Google Safe Browsing	The additional module which is used to enrich the event
GeoIP Country	The additional module which is used to enrich the event
JOE Sandbox	The additional module which is used to enrich the event
Crowdsec	The additional module which is used to enrich the event
GeoIP ASN	The additional module which is used to enrich the event
RBL	The additional module which is used to enrich the event
Yeti	The additional module which is used to enrich the event
OCR Enrich	The additional module which is used to enrich the event
Onyphe	The additional module which is used to enrich the event
ODT Enrich	The additional module which is used to enrich the event
Social Scan	The additional module which is used to enrich the event
Sophos Labs Intelix	The additional module which is used to enrich the event
MMDB Lookup	The additional module which is used to enrich the event
VMRay Submit	The additional module which is used to enrich the event
Trustar Enrich	The additional module which is used to enrich the event
IP Info	The additional module which is used to enrich the event
BackscatterIO	The additional module which is used to enrich the event
IP ASN	The additional module which is used to enrich the event
URL Scan	The additional module which is used to enrich the event
Thread Crowd	The additional module which is used to enrich the event
HTML to Markdown	The additional module which is used to enrich the event
YARA Query	The additional module which is used to enrich the event
Sigma Queries	The additional module which is used to enrich the event
X-Force Exchange	The additional module which is used to enrich the event

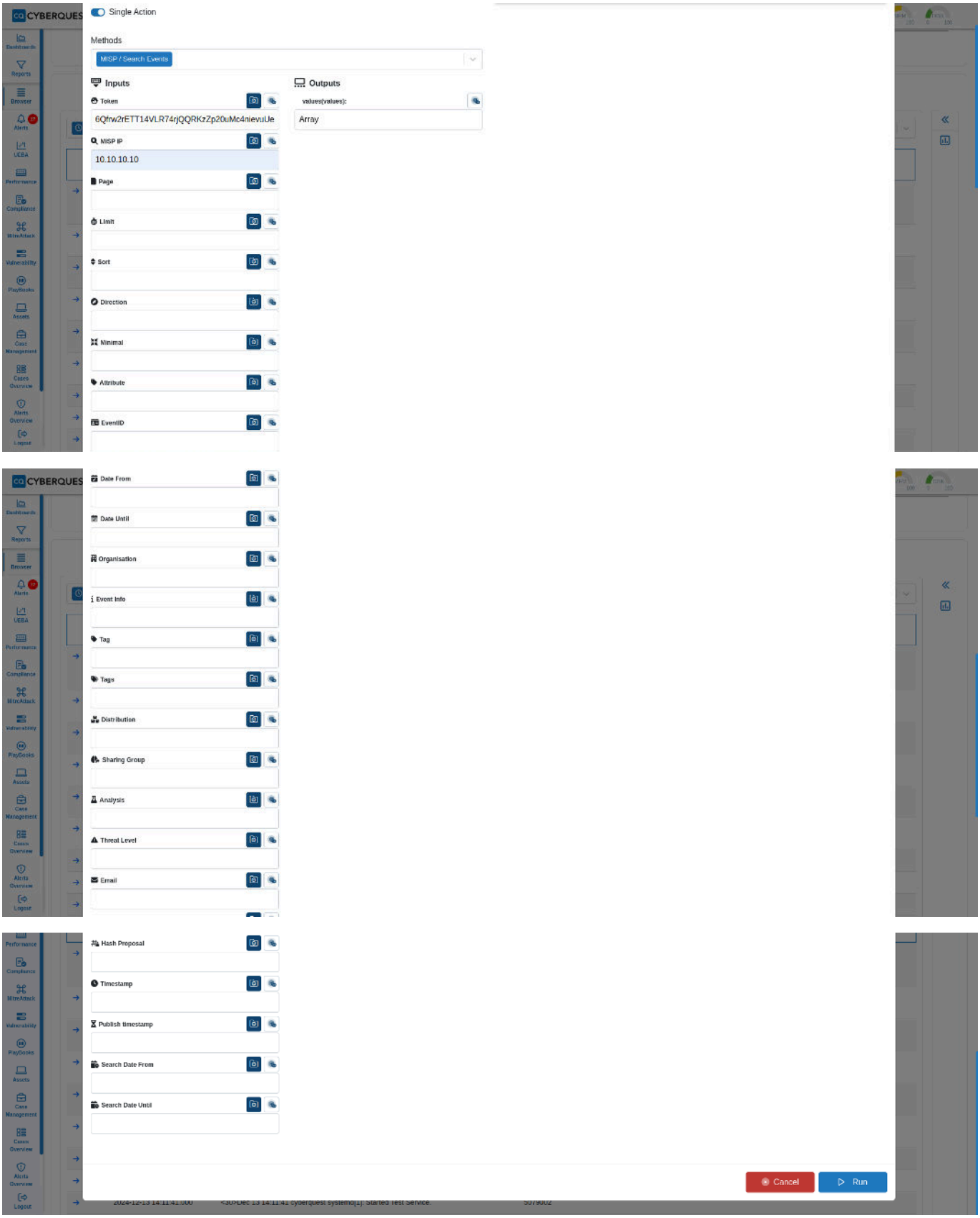
Inputs	Description
WHOIS	The additional module which is used to enrich the event
PDF Enrich	The additional module which is used to enrich the event
Threat Fox	The additional module which is used to enrich the event
Clamav	The additional module which is used to enrich the event
VMware NSX	The additional module which is used to enrich the event
Sigmf	The additional module which is used to enrich the event
URLhaus	The additional module which is used to enrich the event
Stix2 Pattern Syntax Validator	The additional module which is used to enrich the event
Censys Enrich	The additional module which is used to enrich the event
VARIoT DBs	The additional module which is used to enrich the event
JOESandbox Submit	The additional module which is used to enrich the event
Virustotal Public	The additional module which is used to enrich the event
MACAddressIO	The additional module which is used to enrich the event
McAfee Insights Enrich	The additional module which is used to enrich the event
Country Code	The additional module which is used to enrich the event
Shodan	The additional module which is used to enrich the event
DNS DB Query	The additional module which is used to enrich the event
Greynoise	The additional module which is used to enrich the event
XLSX Enrich	The additional module which is used to enrich the event
Lastine Submit	The additional module which is used to enrich the event
Assembly Line Submit	The additional module which is used to enrich the event
Hash Lookup	The additional module which is used to enrich the event
APIVoid	The additional module which is used to enrich the event
Lastline Query	The additional module which is used to enrich the event
EQL	The additional module which is used to enrich the event
Cuckoo submit	The additional module which is used to enrich the event
HYAS Insight	The additional module which is used to enrich the event
Assembly Line Query	The additional module which is used to enrich the event
CIRCL Passive DNS	The additional module which is used to enrich the event
Security Trails	The additional module which is used to enrich the event
Hashdd	The additional module which is used to enrich the event
GeoIP City	The additional module which is used to enrich the event
QRCode	The additional module which is used to enrich the event
Source cache	The additional module which is used to enrich the event
ThreatMiner	The additional module which is used to enrich the event
Cytomic Orion	The additional module which is used to enrich the event
IP Reputation	The additional module which is used to enrich the event
QIntel QSentry	The additional module which is used to enrich the event

Inputs	Description
Wiki	The additional module which is used to enrich the event
CVE	The additional module which is used to enrich the event
BTC Scam Check	The additional module which is used to enrich the event
Whoisfreaks	The additional module which is used to enrich the event
Google Search	The additional module which is used to enrich the event
MalwareBazaar	The additional module which is used to enrich the event
Intel471	The additional module which is used to enrich the event
BTC Steroids	The additional module which is used to enrich the event
Mwdb	The additional module which is used to enrich the event
Dbl Spamhaus	The additional module which is used to enrich the event
Onyphe Full	The additional module which is used to enrich the event
IPqs Fraud and Risk Scoring	The additional module which is used to enrich the event
Farsight Passive DNS	The additional module which is used to enrich the event
CVE Advanced	The additional module which is used to enrich the event
CPE	The additional module which is used to enrich the event
Passive	The additional module which is used to enrich the event
Vulners	The additional module which is used to enrich the event
YARA Syntax Validator	The additional module which is used to enrich the event
Jinja Template Rendering	The additional module which is used to enrich the event
Virustotal	The additional module which is used to enrich the event
MACVendors	The additional module which is used to enrich the event
VulnDB	The additional module which is used to enrich the event
CIRCL Passive SSL	The additional module which is used to enrich the event
DNS	The additional module which is used to enrich the event
OTX	The additional module which is used to enrich the event
Bgpranking	The additional module which is used to enrich the event
Extract URL Components	The additional module which is used to enrich the event
IntelMQ EventDB	The additional module which is used to enrich the event
ApiosintDS	The additional module which is used to enrich the event
PPTX Enrich	The additional module which is used to enrich the event
Hibp	The additional module which is used to enrich the event

Outputs	Description
Saved (saved)	True if the operation was successful, otherwise False
Success (success)	True if the operation was successful, otherwise False
Message (message)	The message about the action which was realised
ID (id)	The ID of the event on which action was realized

MISP/Search Events

Allows users to query and retrieve events based on specific criteria, such as attributes, dates, or event types, making it easier to find relevant cybersecurity information.

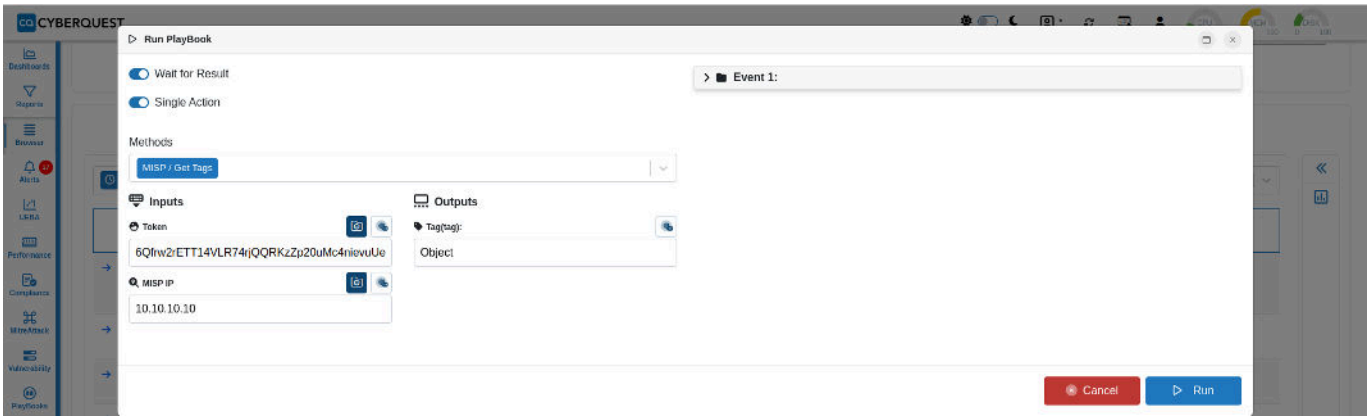


Inputs	Description
Token (is required)	To use the MISP API, you must have an API key
MISP IP (is required)	The IP of the MISP server
Page	Is used for paginating results when retrieving data through the API
Limit	Specifies the maximum number of records to retrieve in a single API response
Sort	Field to be used to sort the result
Direction	Sort direction of the result: asc, desc. Default is asc.
Minimal	Returns a minimal version of the event, only events with attributeCount > 0 will be returned
Attribute	Filter events matching the given string with attributes values
EventID	The ID of the events which is wanted to be searched
Date From	Event creation date is greater or equal
Date Until	Event creation date is less or equal
Organisation	Filter events by matching the creator organisation name
Event Info	Filter events by matching the event info text
Tag	The tag you want to search for
Tags	Filter events by matching any of the event tags of a given list of tag names
Distribution	Who will be able to see this event once it becomes published and eventually when it becomes pulled: 0: Your organization only 1: This community only 2: Connected communities 3: All communities 4: Sharing group 5: Inherit Event
Sharing Group	Specifies the sharing group.It determines the group of users or organizations that have access to the shared data, ensuring controlled and collaborative information sharing.
Analysis	Represents the analysis maturity level. 0: Initial 1: Ongoing 2: Complete
Threat Level	Represents the threat level. 1: High 2: Medium 3: Low 4: Undefined
Email	Filter events by matching the event creator user email
Hash Proposal	Filter events by checking if it has attributes with change proposals. Possible values: 0, 1
Timestamp	Event timestamp greater or equal
Publish timestamp	Represents the date and time when an event or attribute is published, indicating its visibility and availability for sharing with external systems or organizations
Search Date From	Filters on the date, anything newer than the given date in YYYY-MM-DD format is taken.
Search Date Until	Filters on the date, anything older than the given date in YYYY-MM-DD format is taken.

Outputs	Description
values (values)	The results of the API call

MISP/Get Tags

Retrieves a list of tags associated with events, attributes, or other elements, helping users manage and organize their data effectively.

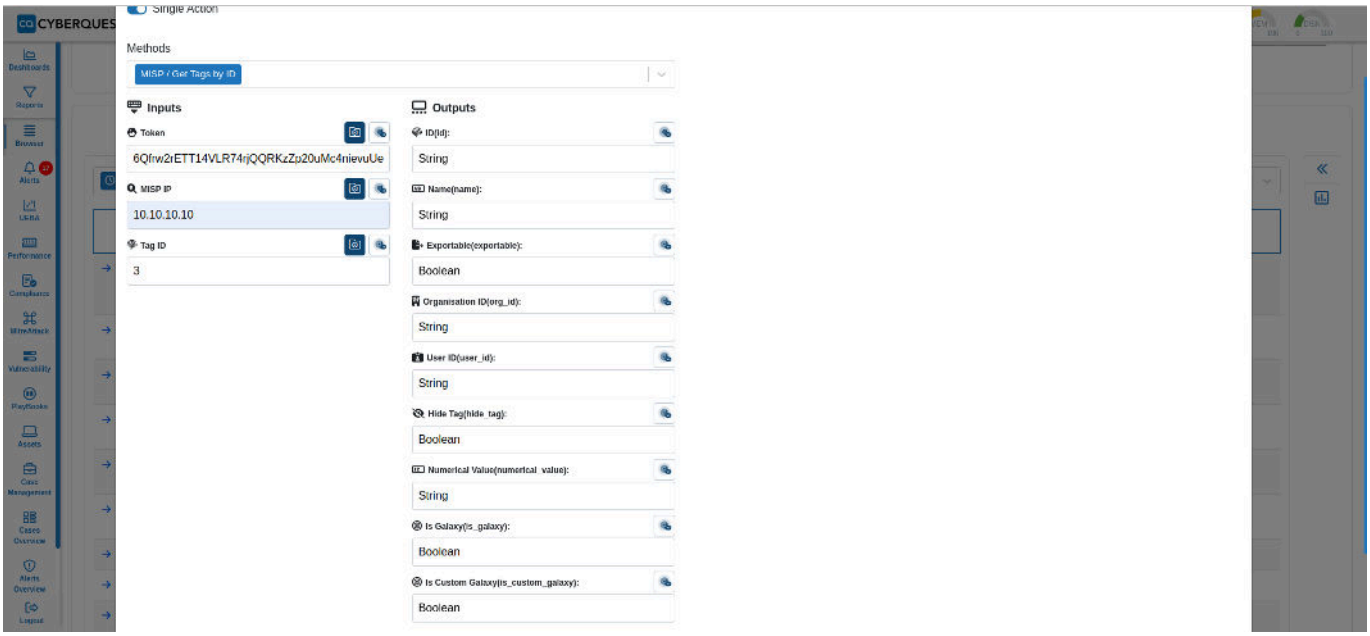


Inputs	Description
Token (is required)	To use the MISP API, you must have an API key
MISP IP (is required)	The IP of the MISP server

Outputs	Description
Tag (tag)	The result of the API call

MISP/Get Tags by ID

Retrieves information about a specific tag using its unique identifier, providing details related to that tags association with events or attribute.

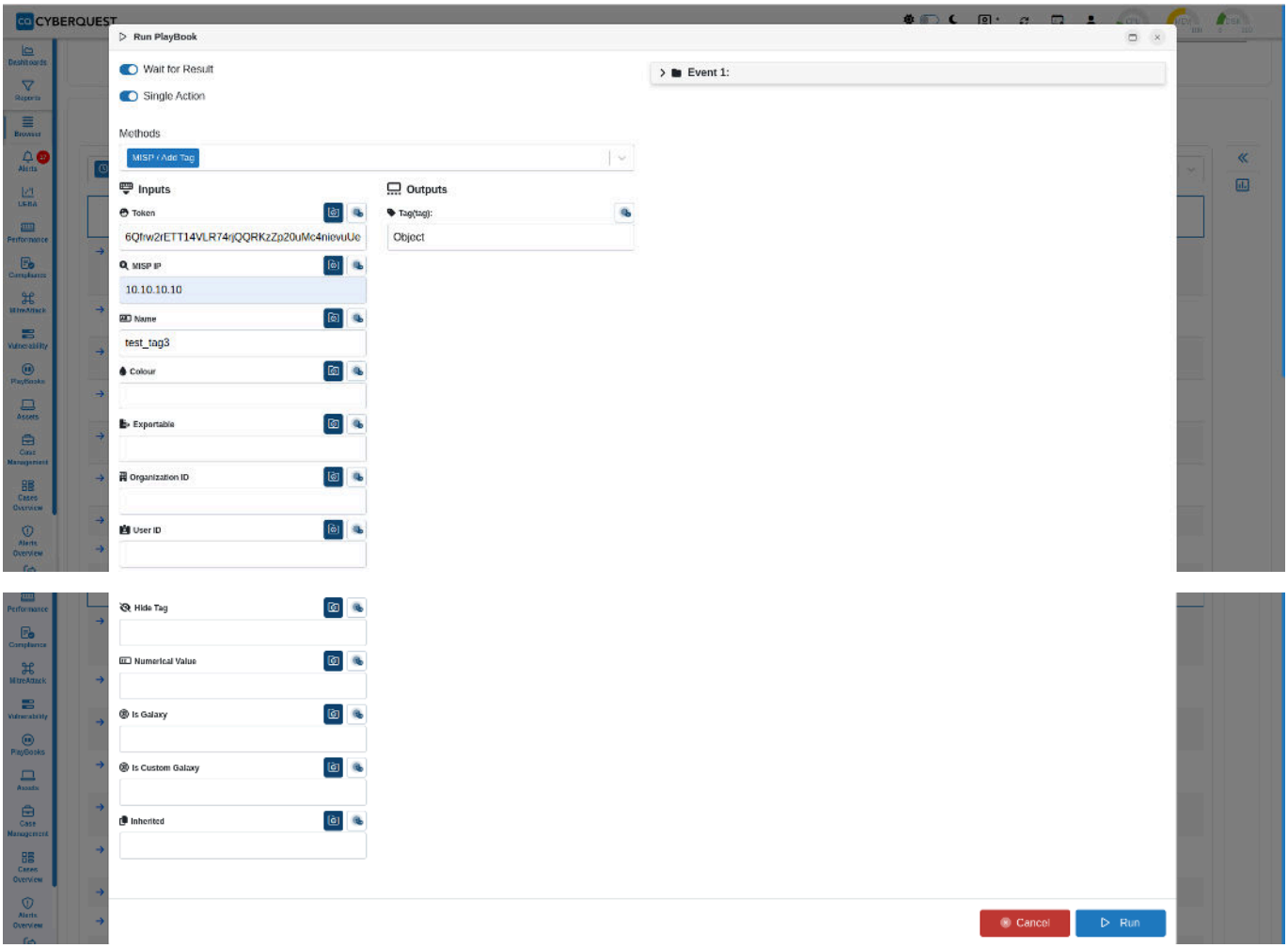


Inputs	Description
Token (is required)	To use the MISP API, you must have an API key
MISP IP (is required)	The IP of the MISP server
Tag ID (is required)	Numeric ID of the tag

Outputs	Description
ID (id)	The ID of the tag on which action was realized
Name (name)	The name of the Tag
Exportable (exportable)	True if the parameter is exportable, otherwise False
Organisation ID (org_id)	It refers to the unique identifier for an organization within the MISP platform
User ID (user_id)	The identification of the user
Hide Tag (hide_tag)	Default value is False
Numerical Value (numerical_value)	Quantitative information about the tag
Is Galaxy (is_galaxy)	Default value is true
Is Custom Galaxy (is_custom_galaxy)	Default value is true

MISP/Add Tag

Allows users to create new tags.

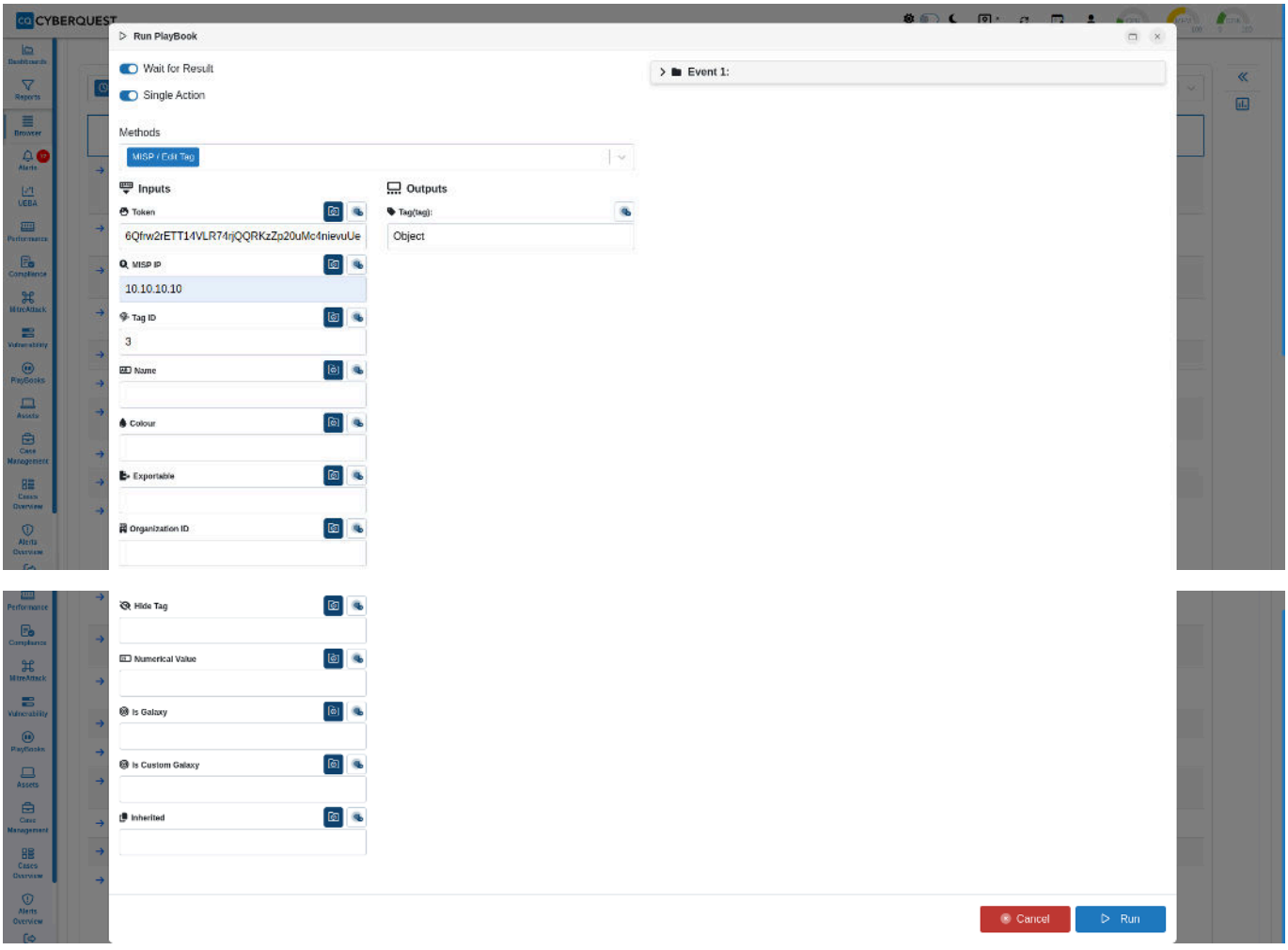


Inputs	Description
Token (is required)	To use the MISP API, you must have an API key
MISP IP (is required)	The IP of the MISP server
Name (is required)	The name of the Tag
Colour	The colour of the tag in MISP interface
Exportable	True if the parameter is exportable, otherwise False
Organization ID	It refers to the unique identifier for an organization within the MISP platform
User ID	The identification of the user
Hide Tag	Default value is False
Numerical Value	Quantitative information about the tag
Is Galaxy	Default value is true
Is Custom Galaxy	Default value is true
Inherited	Default value is 1.

Outputs	Description
Tag (tag)	The tag created

MISP/Edit Tag

Allows users to modify the details of an existing tag, such as its name or associated elements, ensuring accurate and up-to-date categorization within the platform.

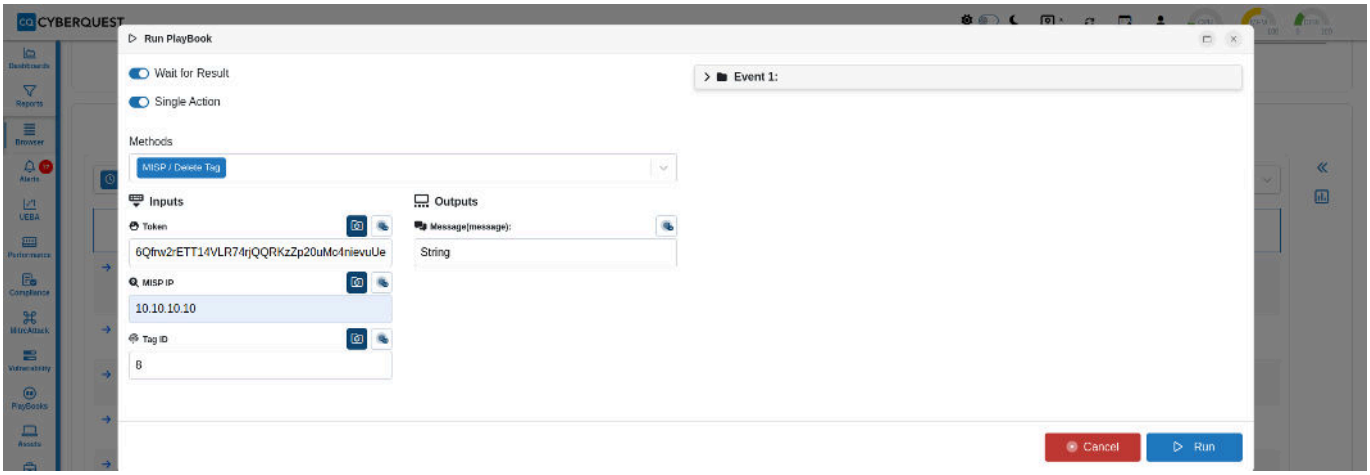


Inputs	Description
Token (is required)	To use the MISP API, you must have an API key
MISP IP (is required)	The IP of the MISP server
Name (is required)	The name of the Tag
Colour	The colour of the tag in MISP interface
Exportable	True if the parameter is exportable, otherwise False
Organization ID	It refers to the unique identifier for an organization within the MISP platform
User ID	The identification of the user
Hide Tag	Default value is False
Numerical Value	Quantitative information about the tag
Is Galaxy	Default value is true
Is Custom Galaxy	Default value is true
Inherited	Default value is 1.

Outputs	Description
Tag (tag)	The tag edited

MISP/Delete Tag

Removes a specific tag from events, attributes, or other elements, helping to manage and clean up unused or outdated tags.

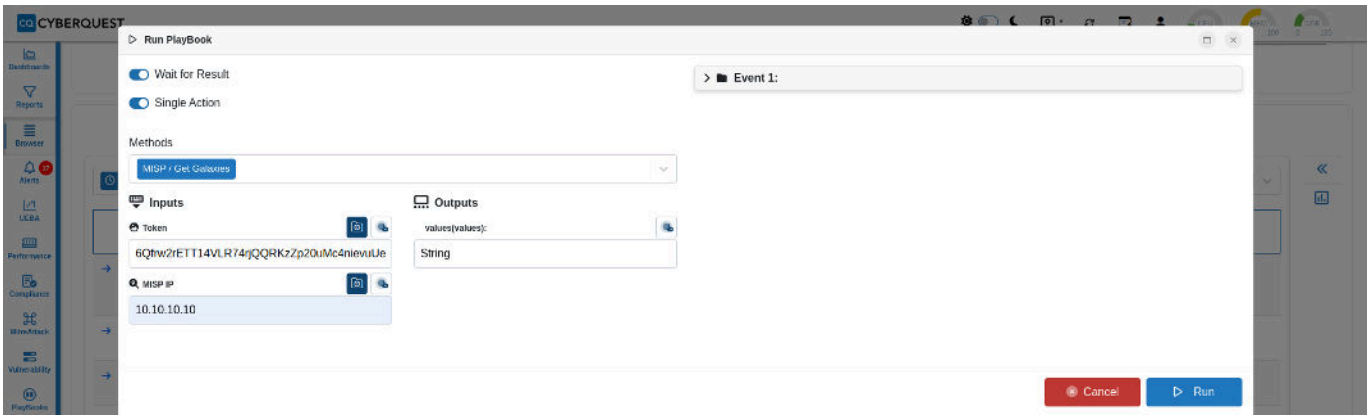


Inputs	Description
Token (is required)	To use the MISP API, you must have an API key
MISP IP (is required)	The IP of the MISP server
Tag ID (is required)	Numeric ID of the attribute

Outputs	Description
Message (message)	The message about the action which was realised

MISP/Get Galaxies

Retrieves a list of galaxy objects, which represent groups of related attributes or data, providing a structured way to organize and manage complex threat intelligence information.

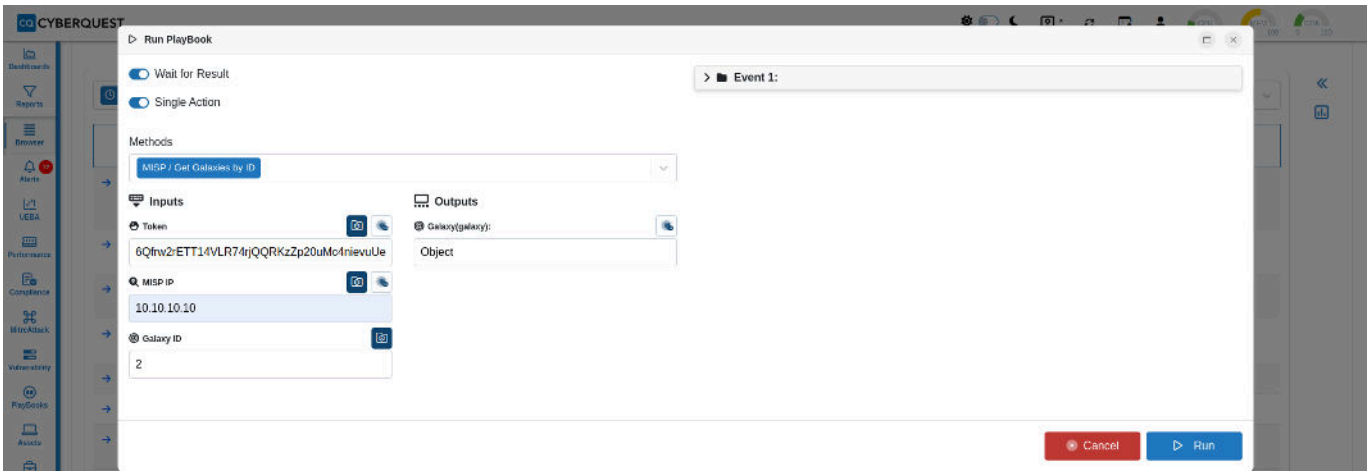


Inputs	Description
Token (is required)	To use the MISP API, you must have an API key
MISP IP (is required)	The IP of the MISP server

Outputs	Description
values (values)	The results of the API call

MISP/Get Galaxies by ID

Retrieves a specific galaxy object using its unique identifier, allowing users to access detailed information about related attributes or data.

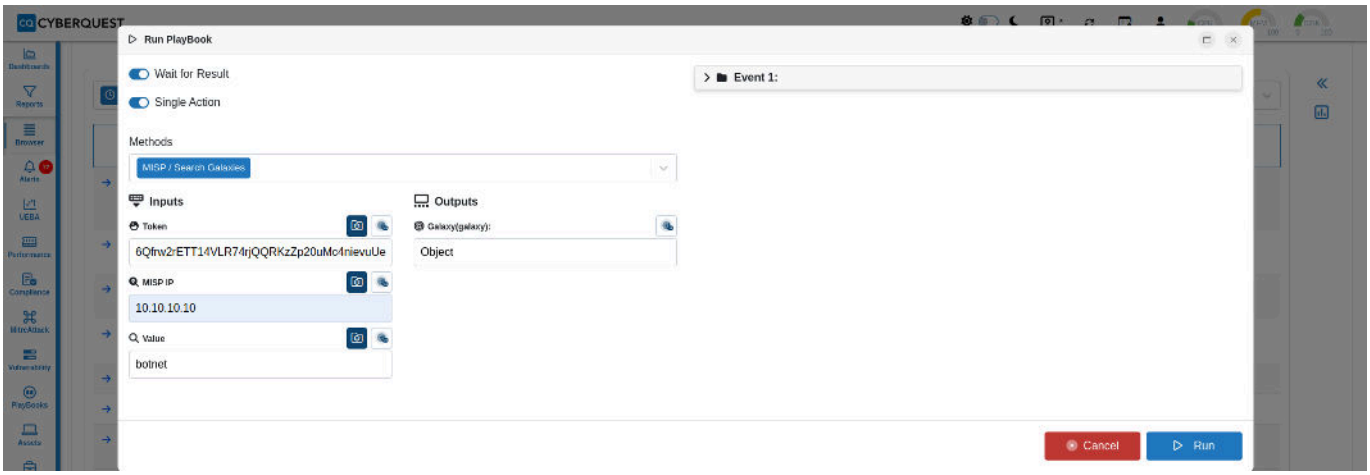


Inputs	Description
Token (is required)	To use the MISP API, you must have an API key
MISP IP (is required)	The IP of the MISP server
Galaxy ID (is required)	

Outputs	Description
Galaxy (galaxy)	The searched galaxy

MISP/Search Galaxies

Allows users to query and retrieve galaxy objects based on specific criteria, helping to organize and manage complex cybersecurity data effectively.

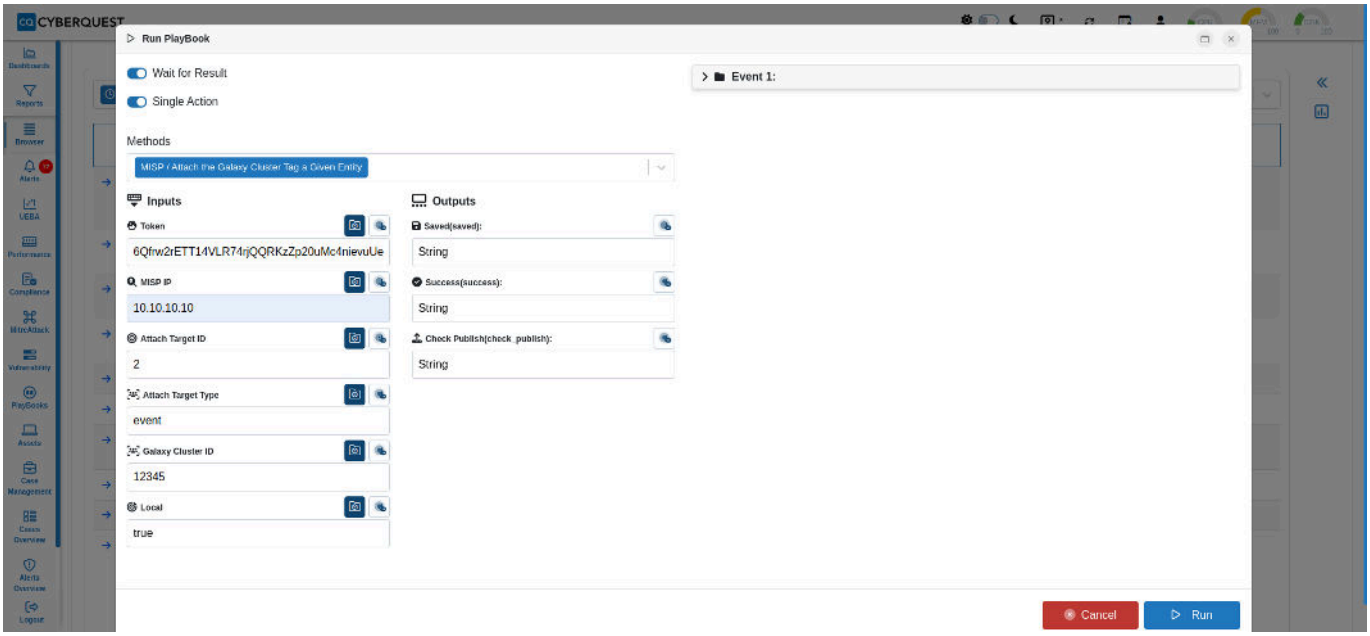


Inputs	Description
Token (is required)	To use the MISP API, you must have an API key
MISP IP (is required)	The IP of the MISP server
Value (is required)	Text search term to find a matching galaxy name, namespace, description, kill_chain_order or uuid.

Outputs	Description
Galaxy (galaxy)	A list of galaxies based of the search criteria

MISP/Attach the Galaxy Cluster Tag a Given Entity

Associates a galaxy cluster tag with a specific event or attribute, enabling the organization and enrichment of related cybersecurity data.

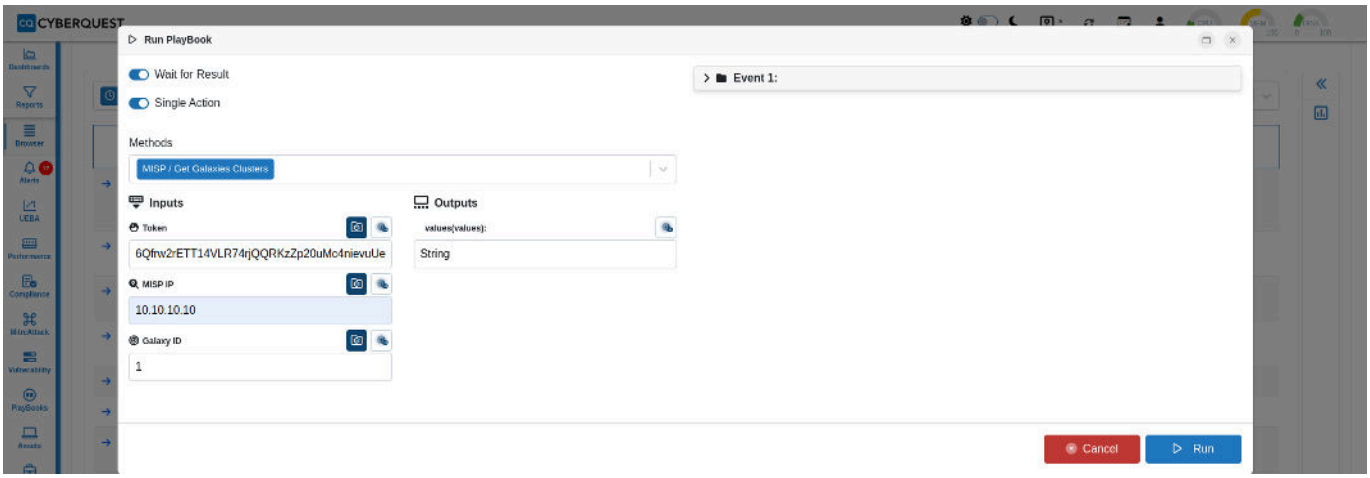


Inputs	Description
Token (is required)	To use the MISP API, you must have an API key
MISP IP (is required)	The IP of the MISP server
Attach Target ID (is required)	UUID or numeric ID of the target entity (Event, Attribute or TagCollection)
Attach Target Type (is required)	Type of the target entity to attach to the galaxy cluster.
Galaxy Cluster ID (is required)	Target galaxy cluster to attach
Local (is required)	Whether the object should be attached locally or not to the target

Outputs	Description
Saved (saved)	True if the operation was successful, otherwise False
Success (success)	True if the operation was successful, otherwise False
Check Publish (check_publish)	Is used to verify whether an event or attribute is ready for publication or sharing.

MISP/Get Galaxies Clusters

Retrieves a list of galaxy clusters, which group related galaxies to help organize and manage complex relationships within cybersecurity data.

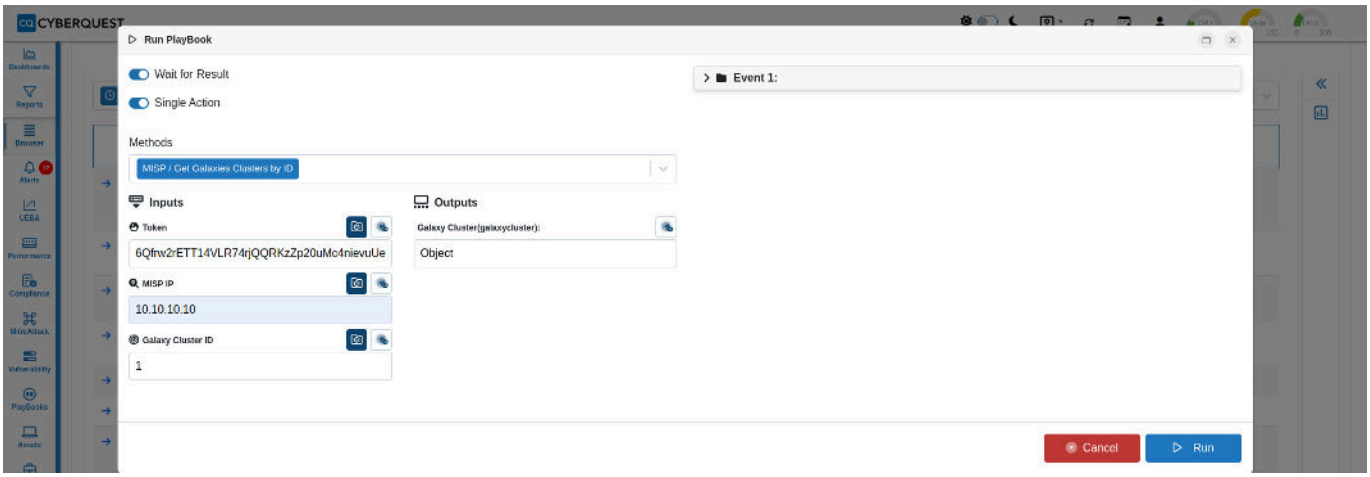


Inputs	Description
Token (is required)	To use the MISP API, you must have an API key
MISP IP (is required)	The IP of the MISP server
Galaxy ID (is required)	UUID or numeric ID of the galaxy

Outputs	Description
values (values)	The results of the API call

MISP/Get Galaxies Clusters by ID

Retrieves details of a specific galaxy cluster using its unique identifier, providing insight into its associated galaxies and data.

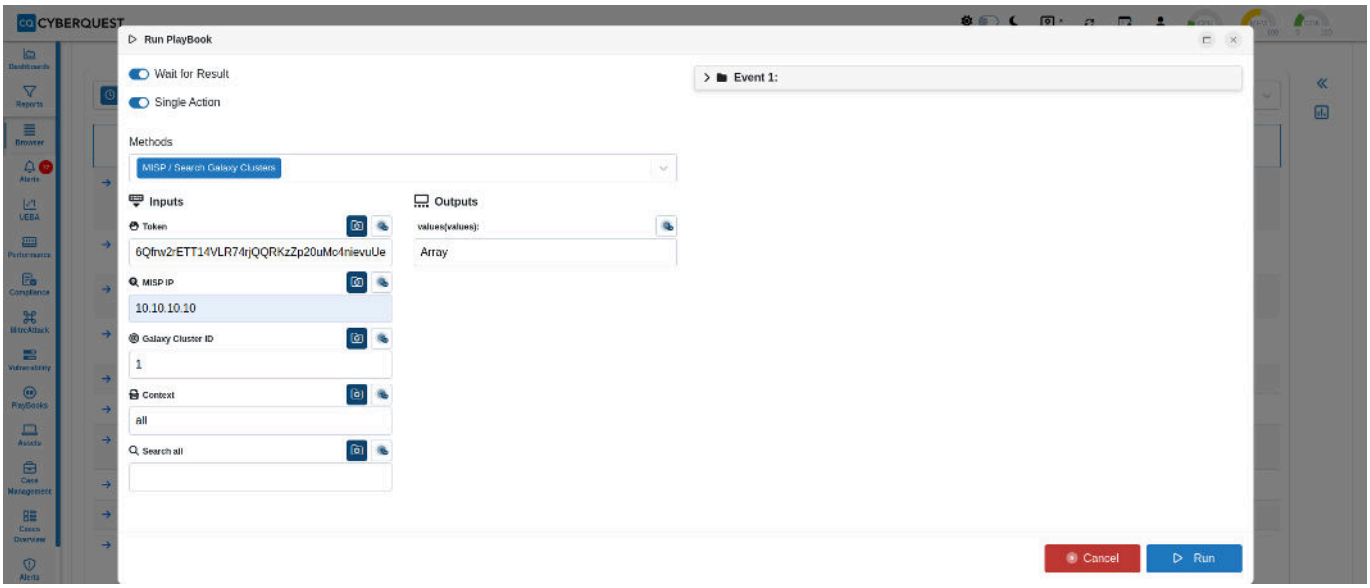


Inputs	Description
Token (is required)	To use the MISP API, you must have an API key
MISP IP (is required)	The IP of the MISP server
Galaxy Cluster ID (is required)	UUID or numeric ID of the galaxy cluster

Outputs	Description
Galaxy Cluster (galaxycluster)	A galaxy cluster with all its details.

MISP/Search Galaxy Clusters

Allows users to search for galaxy clusters based on specific criteria, helping to manage and analyze complex groups of related cybersecurity da.

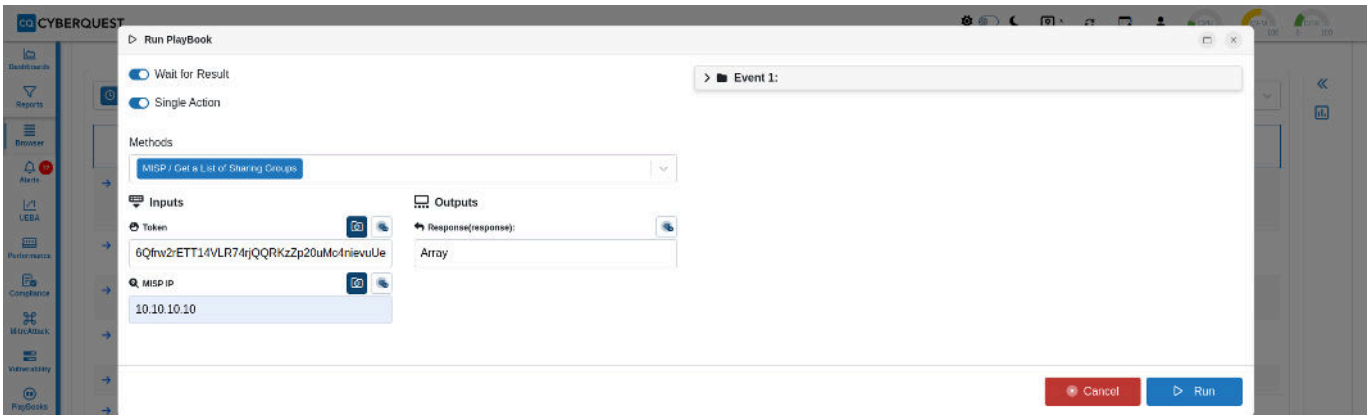


Inputs	Description
Token (is required)	To use the MISP API, you must have an API key
MISP IP (is required)	The IP of the MISP server
Galaxy Cluster ID (is required)	UUID or numeric ID of the galaxy cluster
Context (is required)	Possible values:all, default, org,deleted
Search all	Search galaxy clusters by matching any value, description, uuid or galaxy elements values.

Outputs	Description
values (values)	The results of the API call

MISP/Get a List of Sharing Groups

Retrieves all sharing groups available within the platform, allowing users to manage and organize access to shared threat intelligence.

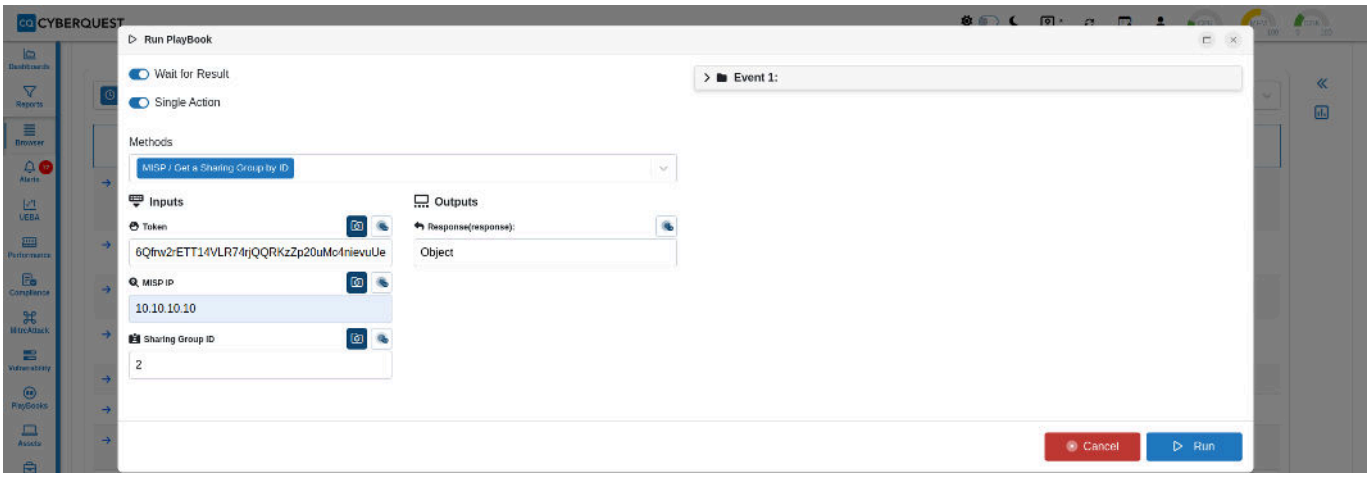


Inputs	Description
Token (is required)	To use the MISP API, you must have an API key
MISP IP (is required)	The IP of the MISP server

Outputs	Description
Response (response)	The list of the Sharing Groups

MISP/Get a Sharing Group by ID

Retrieves details of a specific sharing group using its unique identifier, providing information about its associated events, attributes, and members.

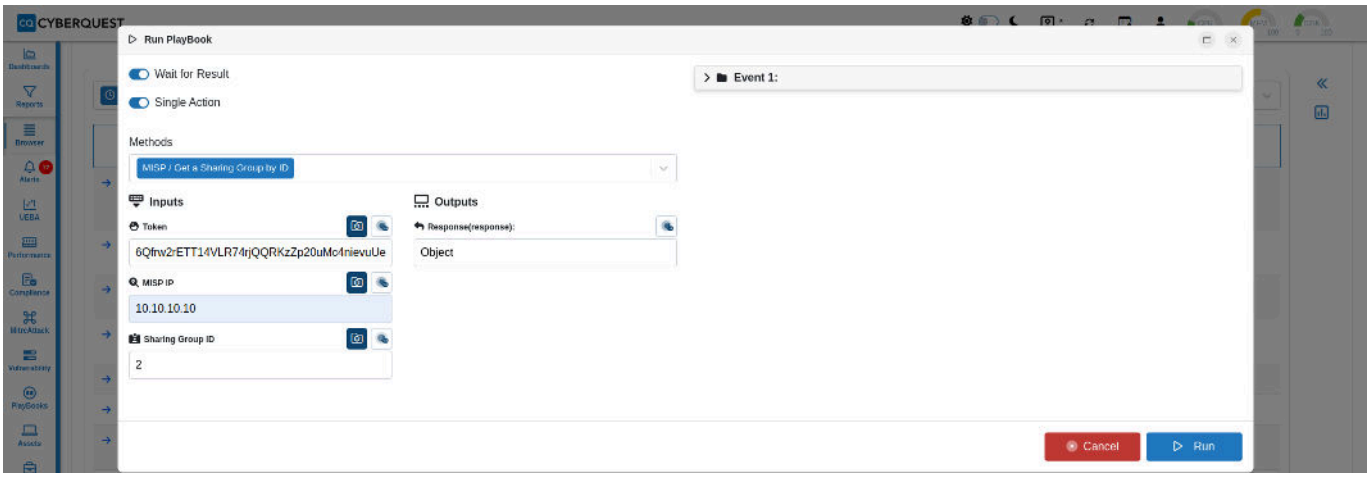


Inputs	Description
Token (is required)	To use the MISP API, you must have an API key
MISP IP (is required)	The IP of the MISP server
Sharing Group ID (is required)	UUID or numeric ID of the sharing group

Outputs	Description
Response (response)	The response of the API call

MISP/Add a Sharing Group

Creates a new sharing group, allowing users to manage collaboration and access to shared cybersecurity information within specific groups.

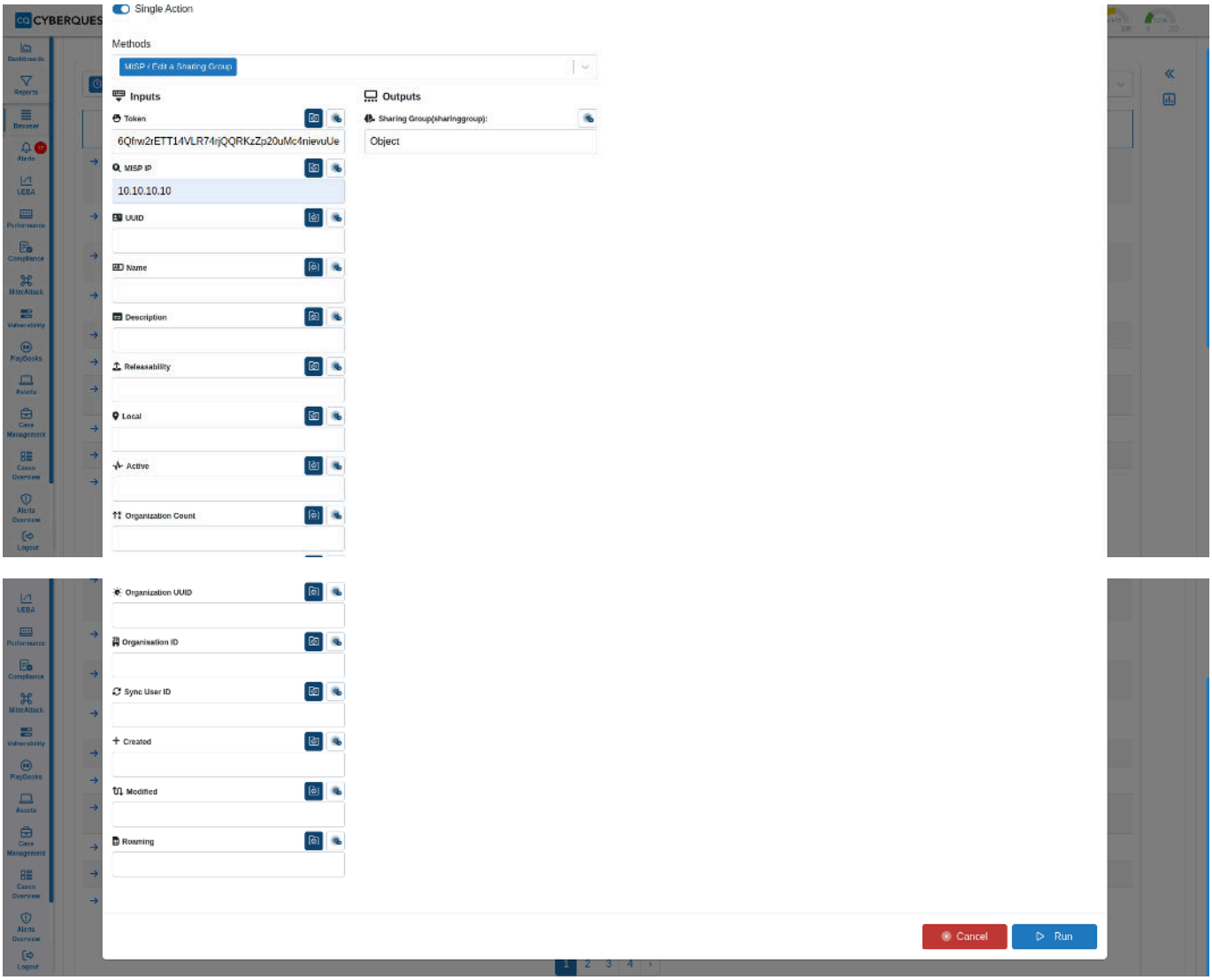


Inputs	Description
Token (is required)	To use the MISP API, you must have an API key
MISP IP (is required)	The IP of the MISP server
UUID	It is a universally unique identifier used to uniquely identify and manage events, attributes, or other objects within the platform. It ensures that each entity is distinct and easily traceable across MISP
Name	The name of the Sharing Group
Description	The short description about the Sharing Group
Releasability	Defines the conditions or restrictions for the Sharing Group
Local	True if the Sharing Group is local, otherwise False
Active	True if the Sharing Group is false, otherwise false
Organization Count	Indicates the number of the organisation in MISP
Organization UUID	UUID of the Organisation
Organisation ID	It refers to the unique identifier for an organization within the MISP platform
Sync User ID	The user ID responsible for the Sharing Group
Created	The date of creation
Modified	The date of the modifications
Roaming	True if the Sharing Group is not locally

Outputs	Description
Sharing Group (sharinggroup)	The new created Sharing Group

MISP/Edit a Sharing Group

Allows users to modify details of an existing sharing group, such as its name, members, or access permissions, to ensure proper management of shared data.

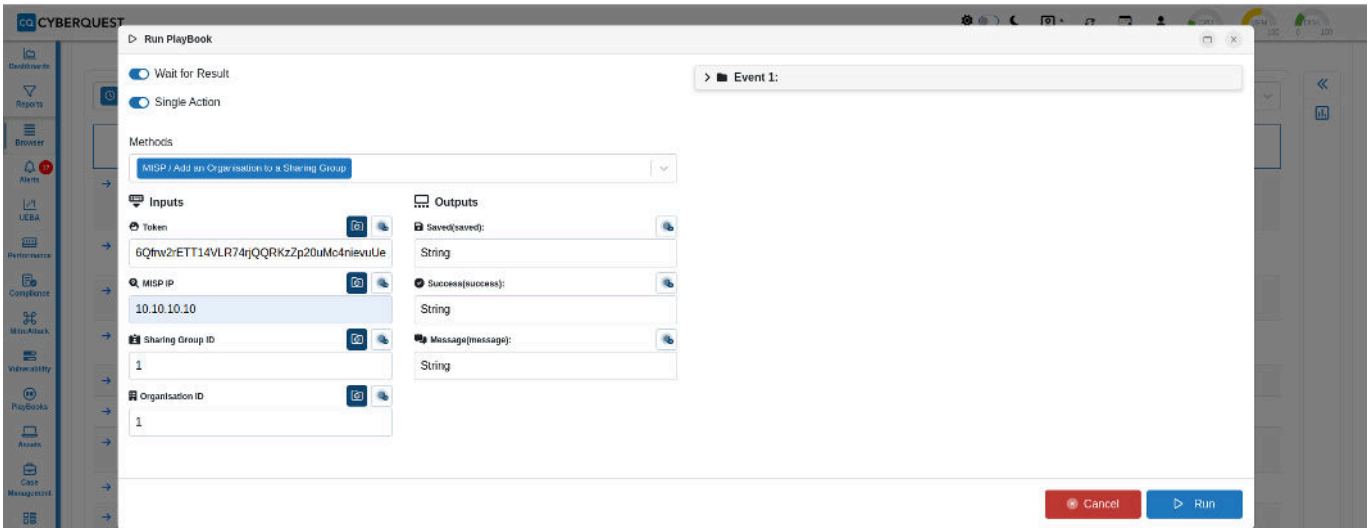

Single Action
Methods
MISP / Edit a Sharing Group
Inputs
Token
6Qfrw2rETT14VLR74rjQQRKzZp20uMc4nievuUe
MISP IP
10.10.10.10
UUID
Name
Description
Releasability
Local
Active
Organization Count
Outputs
Sharing Group(sharinggroup):
Object
Organization UUID
Organisation ID
Sync User ID
Created
Modified
Roaming
Cancel
Run

Inputs	Description
Token (is required)	To use the MISP API, you must have an API key
MISP IP (is required)	The IP of the MISP server
UUID	It is a universally unique identifier used to uniquely identify and manage events, attributes, or other objects within the platform. It ensures that each entity is distinct and easily traceable across MISP
Name	The name of the Sharing Group
Description	The short description about the Sharing Group
Releasability	Defines the conditions or restrictions for the Sharing Group
Local	True if the Sharing Group is local, otherwise False
Active	True if the Sharing Group is false, otherwise false
Organization Count	Indicates the number of the organisation in MISP
Organization UUID	UUID of the Organisation
Organisation ID	It refers to the unique identifier for an organization within the MISP platform
Sync User ID	The user ID responsible for the Sharing Group
Created	The date of creation
Modified	The date of the modifications
Roaming	True if the Sharing Group is not locally

Outputs	Description
Sharing Group (sharinggroup)	The result of the API call

MISP/Add an Organisation to a Sharing Group

Allows users to associate a specific organization with a sharing group, enabling controlled access and collaboration within the group.

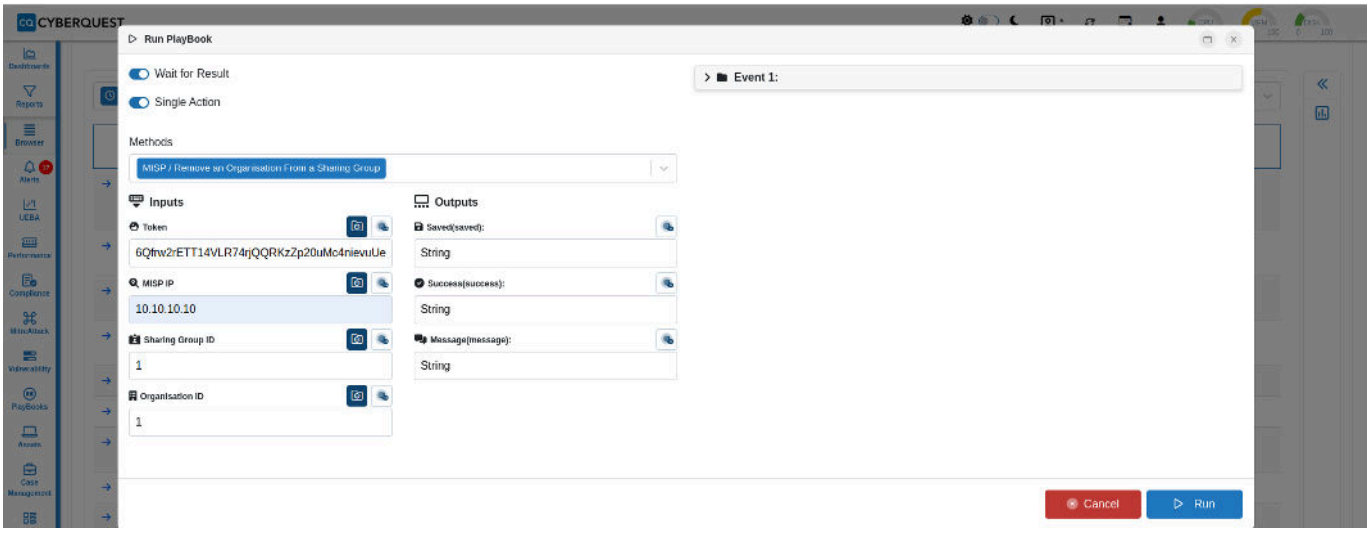


Inputs	Description
Token (is required)	To use the MISP API, you must have an API key
MISP IP (is required)	The IP of the MISP server
Sharing Group ID (is required)	UUID or numeric ID of the sharing group
Organisation ID (is required)	UUID or numeric ID of the organisation

Outputs	Description
Saved (saved)	True if the operation was successful, otherwise False
Success (success)	True if the operation was successful, otherwise False
Message (message)	The message about the action which was realised

MISP/Remove an Organisation From a Sharing Group

Removes an organization from a specific sharing group, managing the collaboration and access to shared data accordingly.

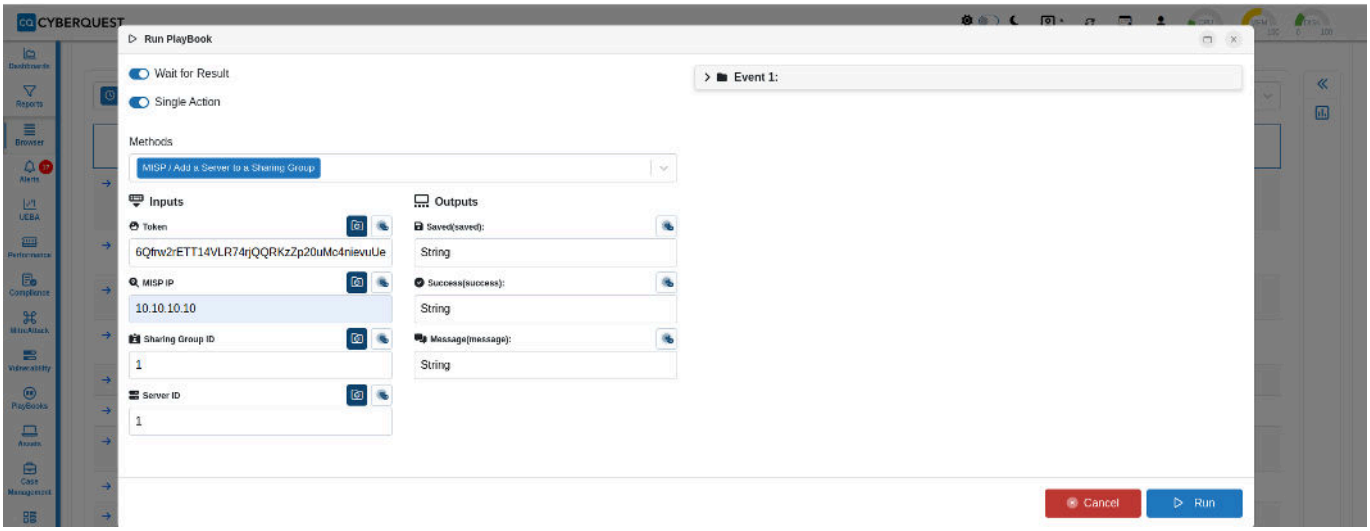


Inputs	Description
Token (is required)	To use the MISP API, you must have an API key
MISP IP (is required)	The IP of the MISP server
Sharing Group ID (is required)	UUID or numeric ID of the sharing group
Organisation ID (is required)	UUID or numeric ID of the organisation

Outputs	Description
Saved (saved)	True if the operation was successful, otherwise False
Success (success)	True if the operation was successful, otherwise False
Message (message)	The message about the action which was realised

MISP/Add a Server to a Sharing Group

Allows users to associate a server with a specific sharing group, enabling secure sharing and management of threat intelligence across that group.

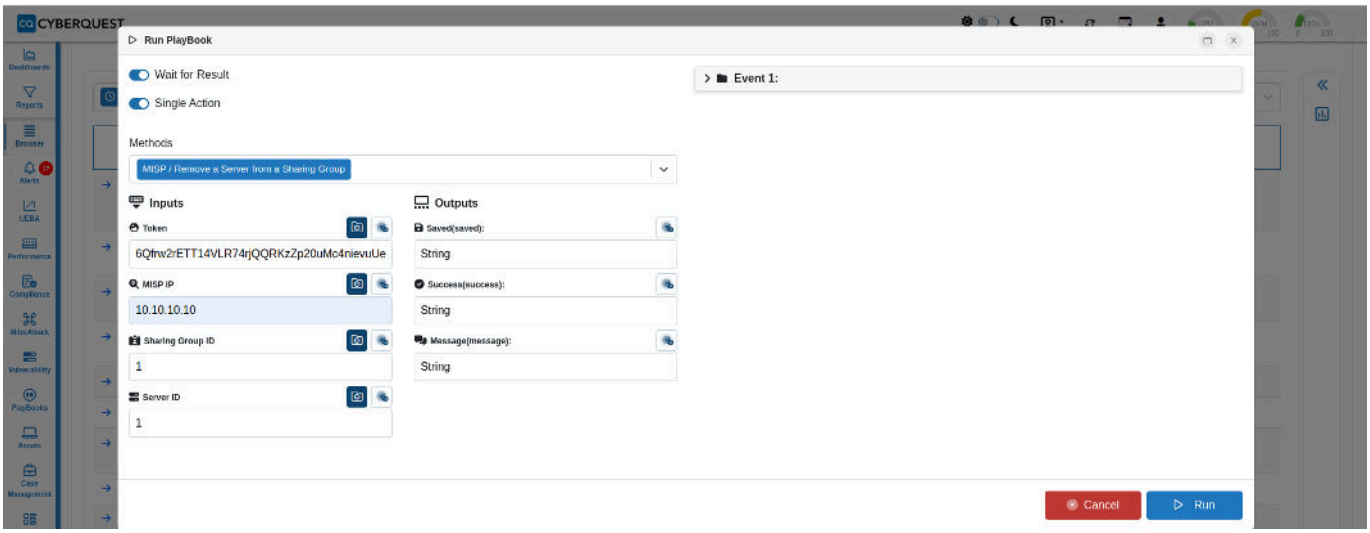


Inputs	Description
Token (is required)	To use the MISP API, you must have an API key
MISP IP (is required)	The IP of the MISP server
Sharing Group ID (is required)	UUID or numeric ID of the sharing group
Server ID (is required)	UUID or numeric ID of the server

Outputs	Description
Saved (saved)	True if the operation was successful, otherwise False
Success (success)	True if the operation was successful, otherwise False
Message (message)	The message about the action which was realised

MISP/Remove a Server from a Sharing Group

Removes a server from a specific sharing group, ensuring proper management and access control for shared data

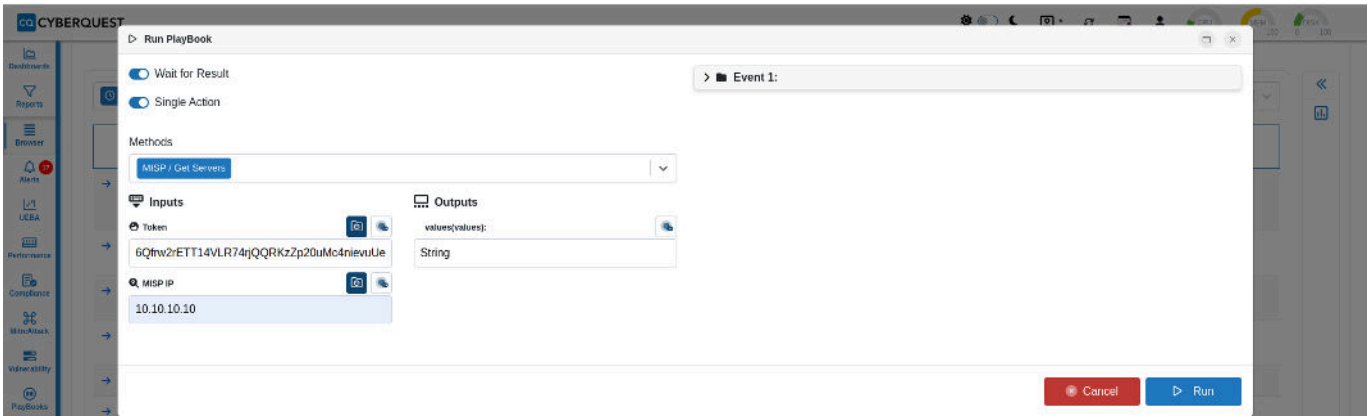


Inputs	Description
Token (is required)	To use the MISP API, you must have an API key
MISP IP (is required)	The IP of the MISP server
Sharing Group ID (is required)	UUID or numeric ID of the sharing group
Server ID (is required)	UUID or numeric ID of the server

Outputs	Description
Saved (saved)	True if the operation was successful, otherwise False
Success (success)	True if the operation was successful, otherwise False
Message (message)	The message about the action which was realised

MISP/Get Servers

Retrieves a list of all servers associated with the platform, providing information on their status, configurations, and sharing group affiliations.

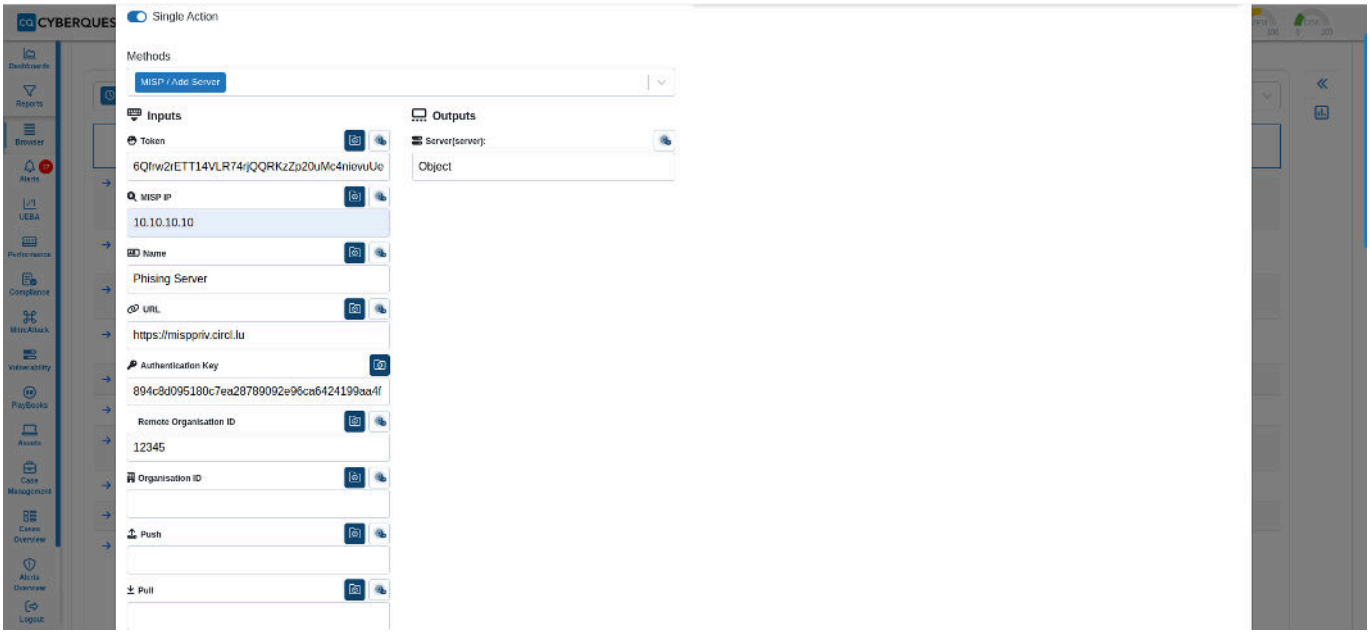


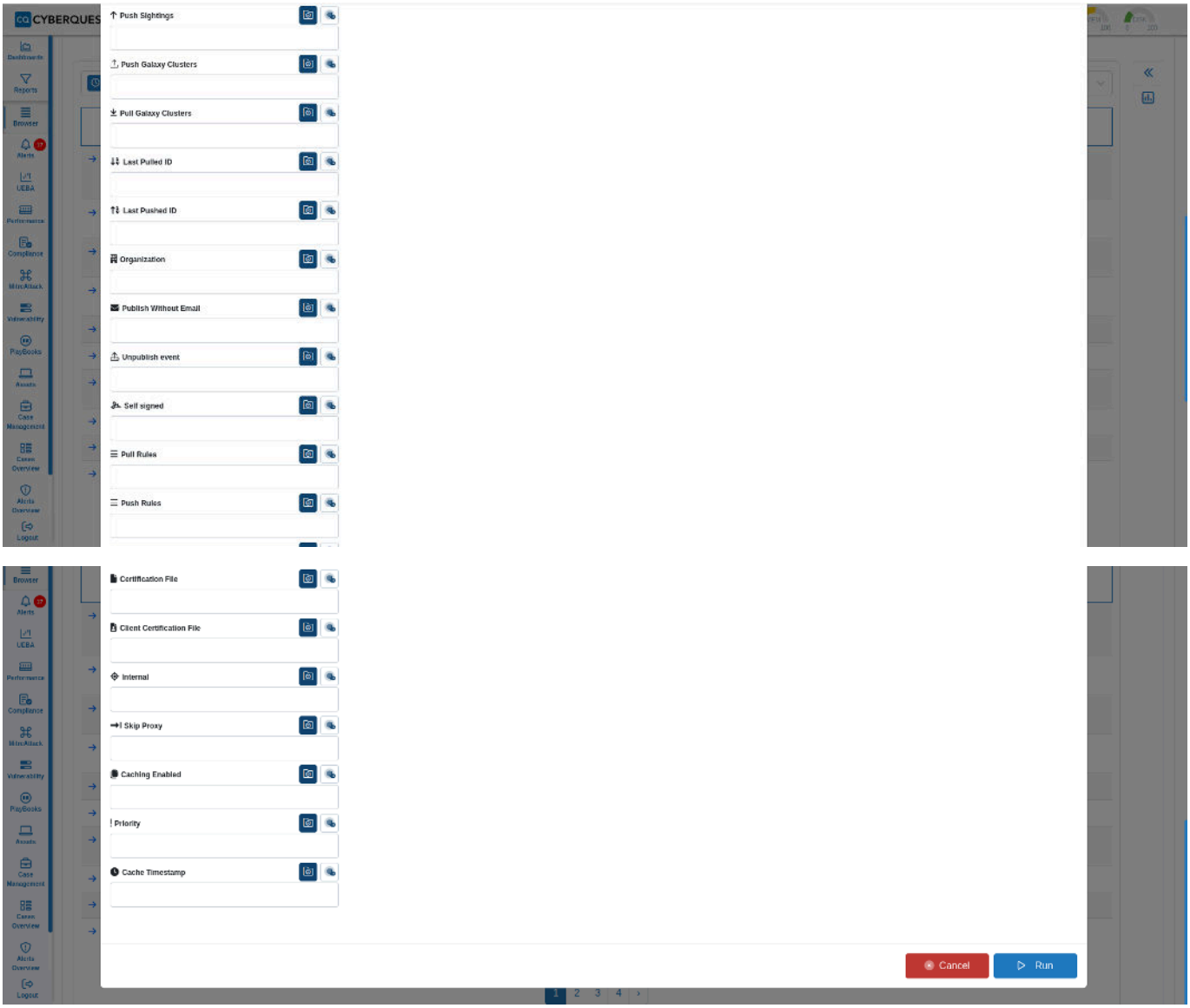
Inputs	Description
Token (is required)	To use the MISP API, you must have an API key
MISP IP (is required)	The IP of the MISP server

Outputs	Description
values (values)	The results of the API call

MISP/Add Server

Allows users to add a new server to the platform, enabling secure sharing and management of threat intelligence.



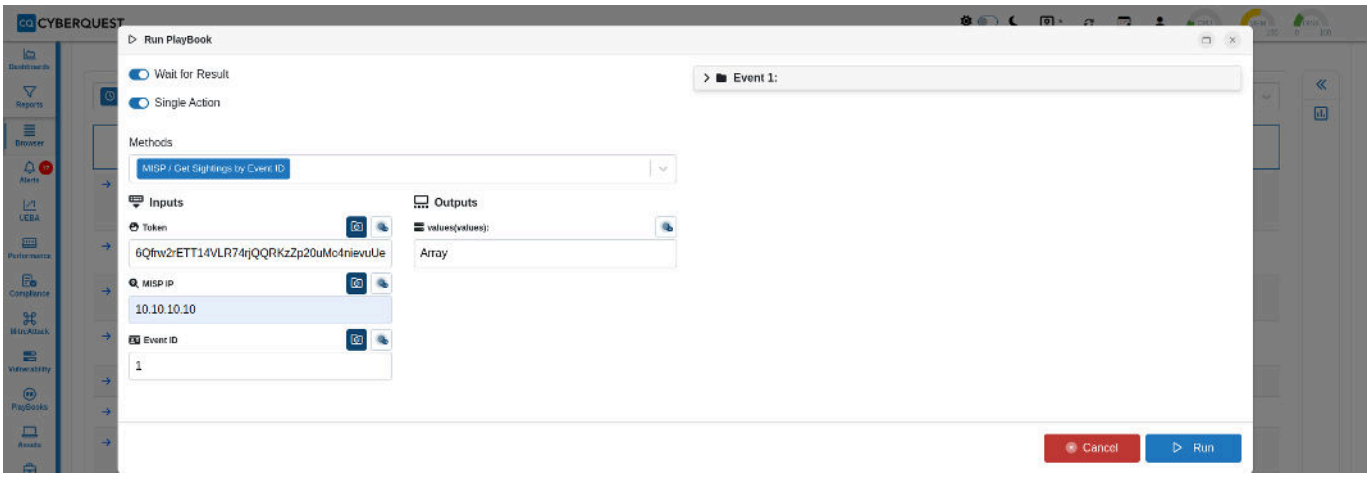

Push Sightings
Push Galaxy Clusters
Pull Galaxy Clusters
Last Pulled ID
Last Pushed ID
Organization
Publish Without Email
Unpublish event
Self signed
Pull Rules
Push Rules
Certification File
Client Certification File
Internal
Skip Proxy
Caching Enabled
Priority
Cache Timestamp
Cancel
Run

Inputs	Description
Token (is required)	To use the MISP API, you must have an API key
MISP IP (is required)	The IP of the MISP server
Name (is required)	The name of the Server
URL (is required)	The IP where the server it is found
Authentication Key (is required)	
Remote Organisation ID (is required)	It refers to the unique identifier for an remote organization within the MISP platform
Organisation ID	It refers to the unique identifier for an organization within the MISP platform
Push	True if the server will pe user to push data
Pull	True if the server will pe user to pull data
Push Sightings	True if the server will pe user to push sightings data
Push Galaxy Clusters	True if the server will pe user to push galaxy clusters data
Pull Galaxy Clusters	True if the server will pe user to pull galaxy clusters data
Last Pulled ID	Tracks the identifier of the last object or event retrieved during a data pull.
Last Pushed ID	Tracks the identifier of the last object or event retrieved during a data push.
Organization	The ID of the organisation
Publish Without Email	Allows an event to be published without triggering a notification email to the users. It is useful for silent updates or when email notifications are unnecessary.
Unpublish event	True if you want to unpublish events
Self signed	True if self signet certificates
Pull Rules	Stringified JSON rules for pulling events from this server.
Push Rules	Stringified JSON rules for pushing events from this server.
Certification File	Base64 encoded certificate
Client Certification File	Base64 encoded client certificate
Internal	True if the server is internal, otherwise false
Skip Proxy	True if you want to skip proxy server, otherwise false
Caching Enabled	True if you want to cache informations, otherwise false
Priority	The priority of the server
Cache Timestamp	True if you want to cache timestamp, otherwise false

Outputs	Description
Server (server)	Informations about new server added

MISP/Get Sightings by Event ID

Retrieves a list of sightings associated with a specific event, providing insights into where and how the event has been observed.

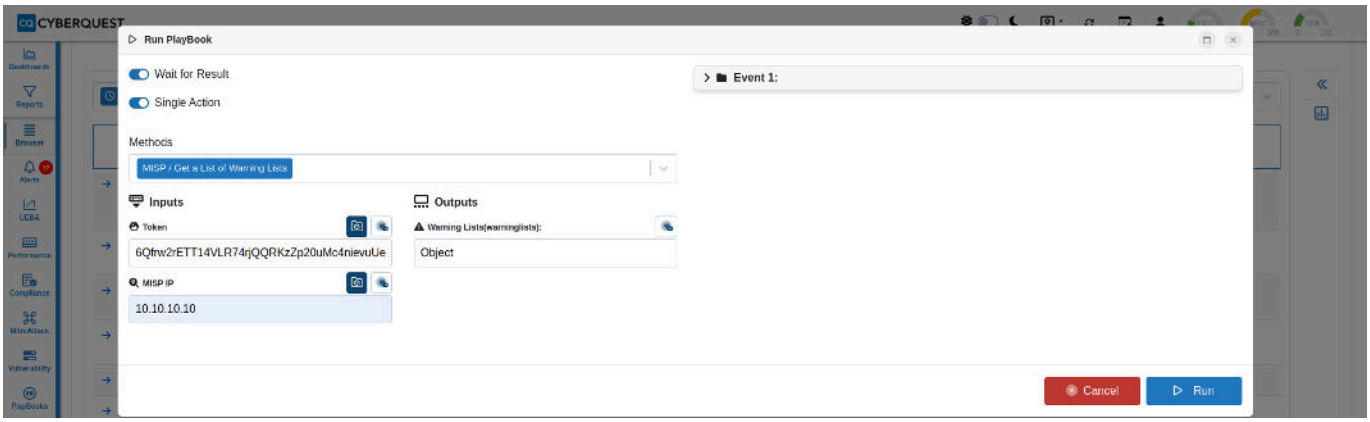


Inputs	Description
Token (is required)	To use the MISP API, you must have an API key
MISP IP (is required)	The IP of the MISP server
Event ID (is required)	The ID of the event which is wanted to be searched

Outputs	Description
values (values)	The results of the API call

MISP/Get a List of Warning Lists

Retrieves all warning lists available, which contain predefined indicators or threat data used to manage and track high-risk entities.

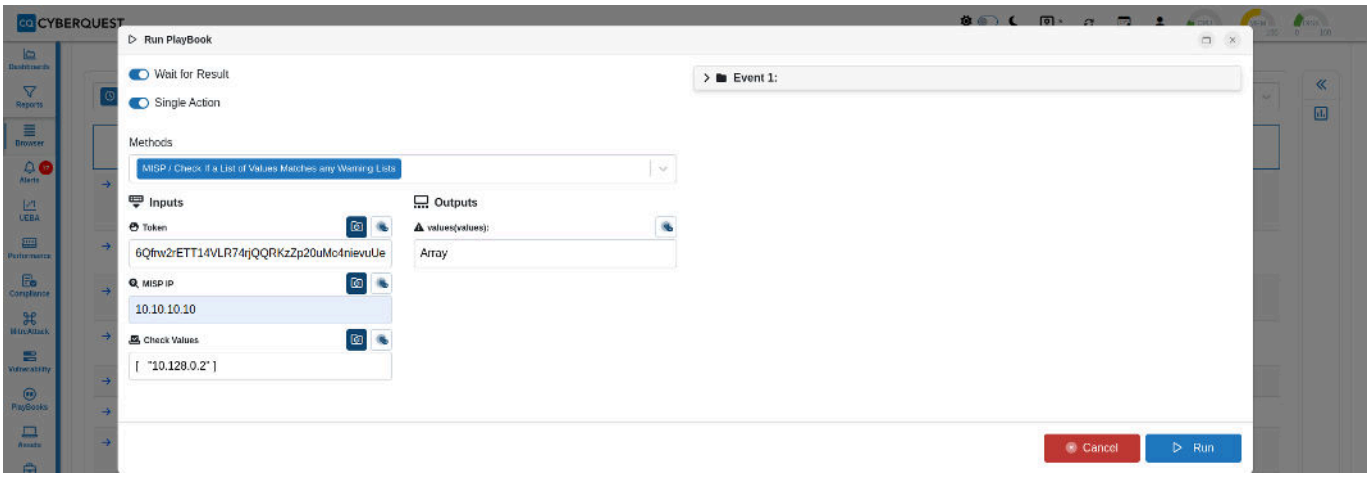


Inputs	Description
Token (is required)	To use the MISP API, you must have an API key
MISP IP (is required)	The IP of the MISP server

Outputs	Description
Warning Lists (warninglists)	The result of the API call

MISP/Check If a List of Values Matches any Warning Lists

Checks a given list of values (e.g., IP addresses, domains) against predefined warning lists to identify potential threats or risky entities.



Inputs	Description
Token (is required)	To use the MISP API, you must have an API key
MISP IP (is required)	The IP of the MISP server
Check Values (is required)	The values you want to check in MISP

Outputs	Description
values (values)	The results of the API call

OS Installation

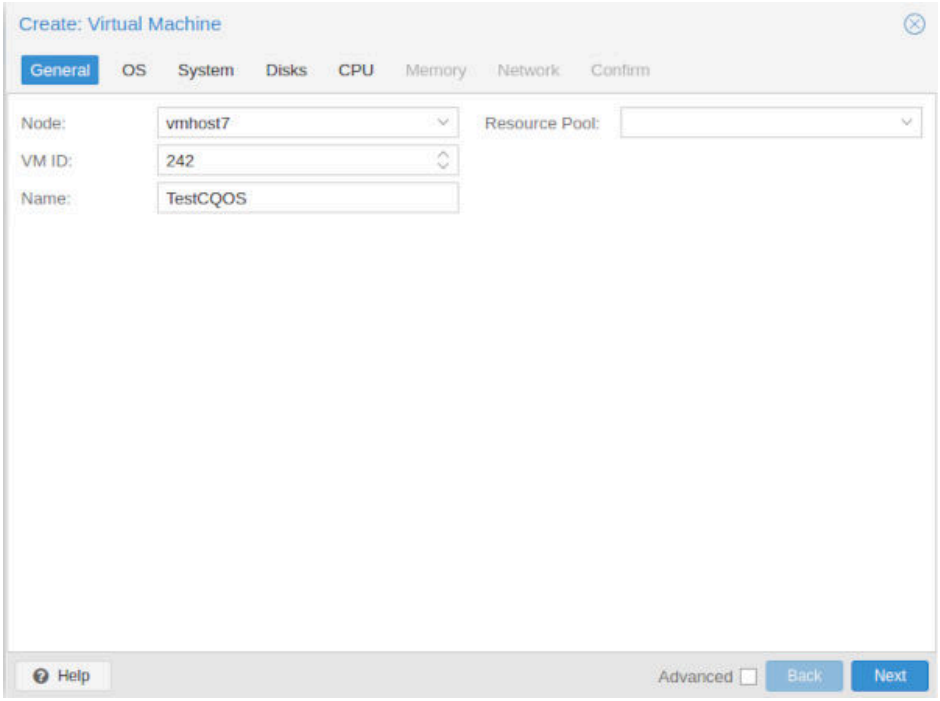
Proxmox Installation

Log in to the Proxmox Web Interface

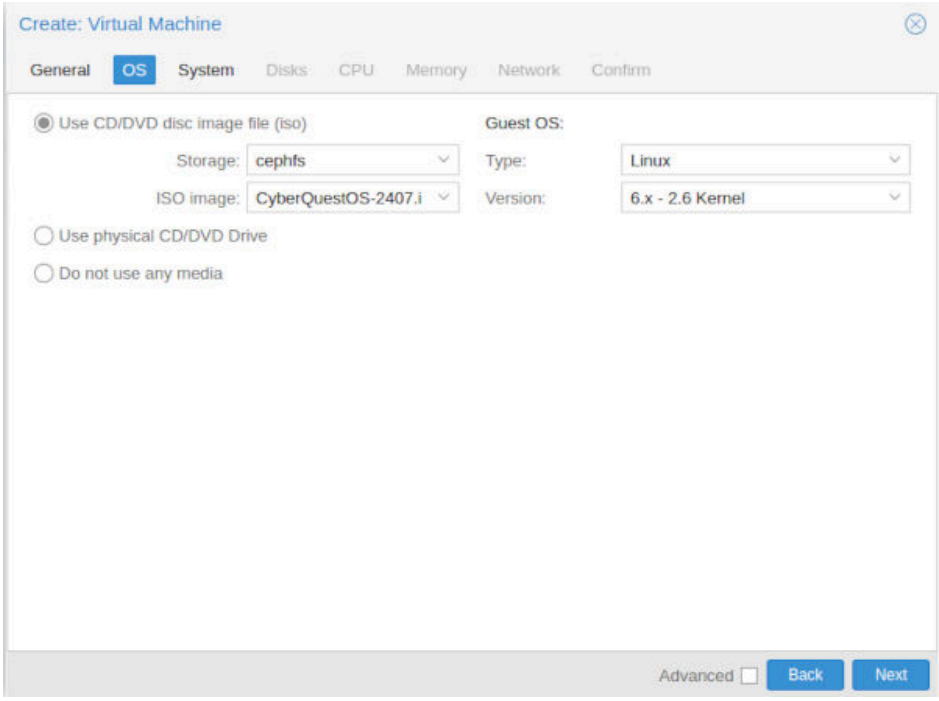
Log in to the Proxmox Web Interface: Use the credentials set during installation.

Create a New VM

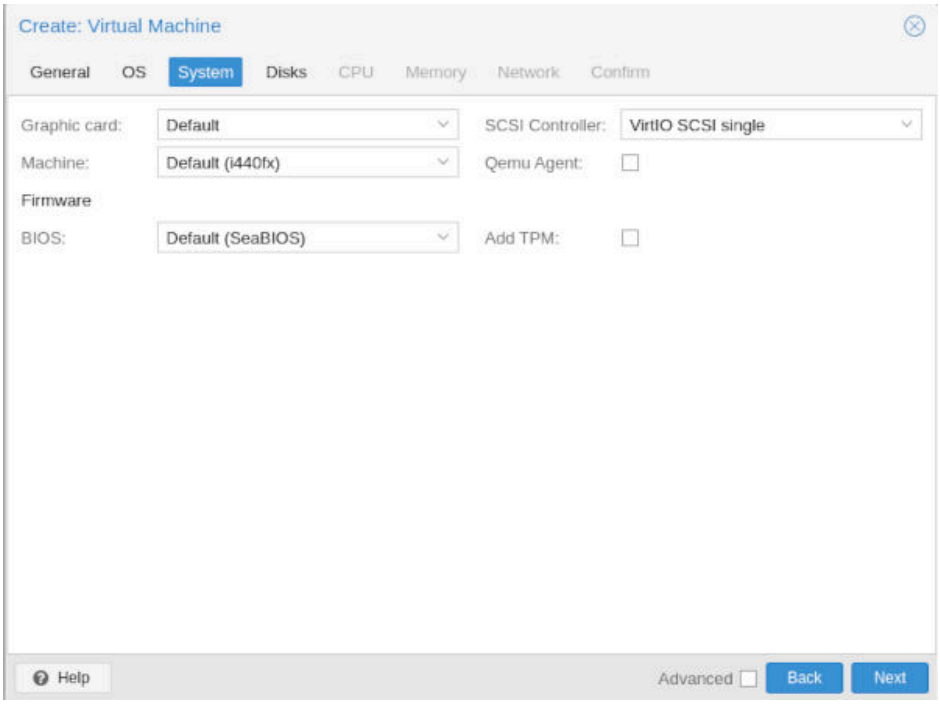
- Click on “Create VM” in the top right corner.
- Enter a VM ID and name.



- Choose the storage location for the ISO image and the CD.



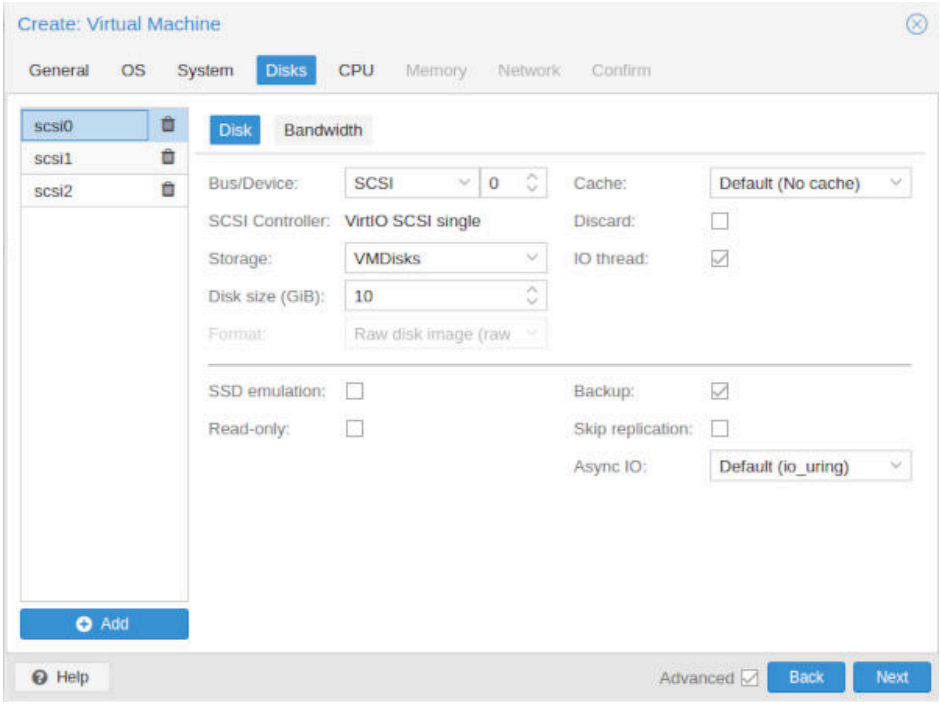
- Configure the “System” settings (BIOS, SCSI Controller, etc.).



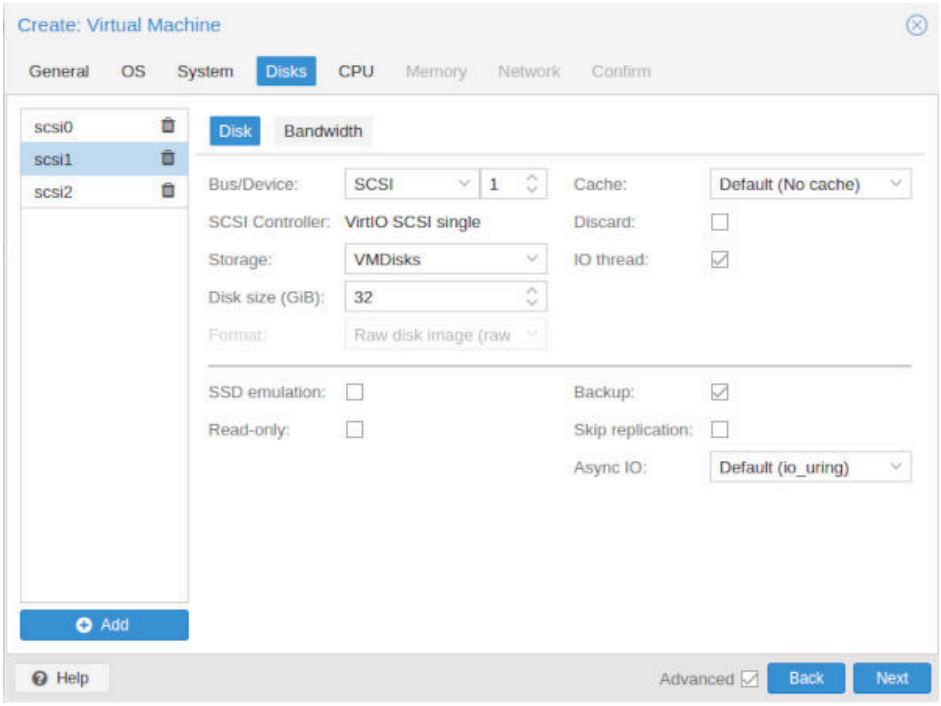
- Configure three disk partitions.

  The recommended setup is:

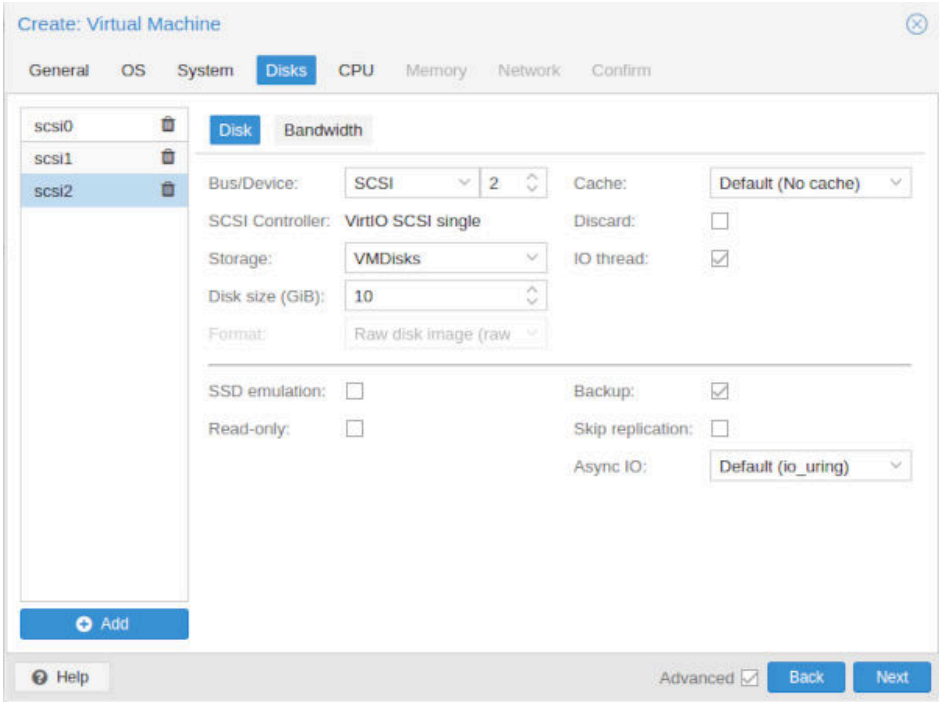
  - scsi0 - 10 GB (where the Operating System will be installed)



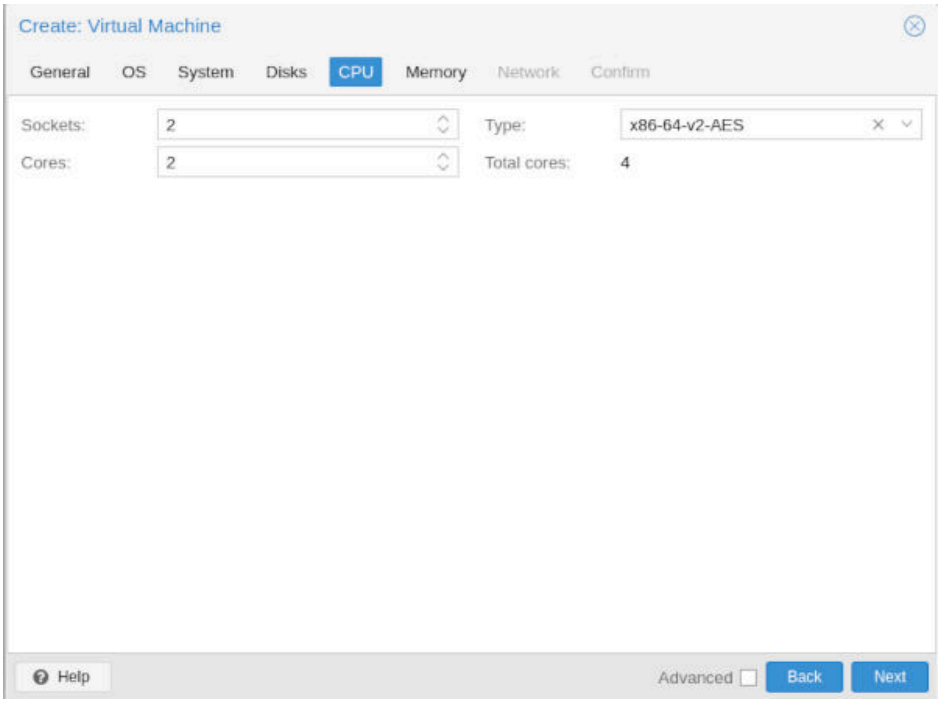
- scsi1 - 32 GB (where the Docker containers are stored)

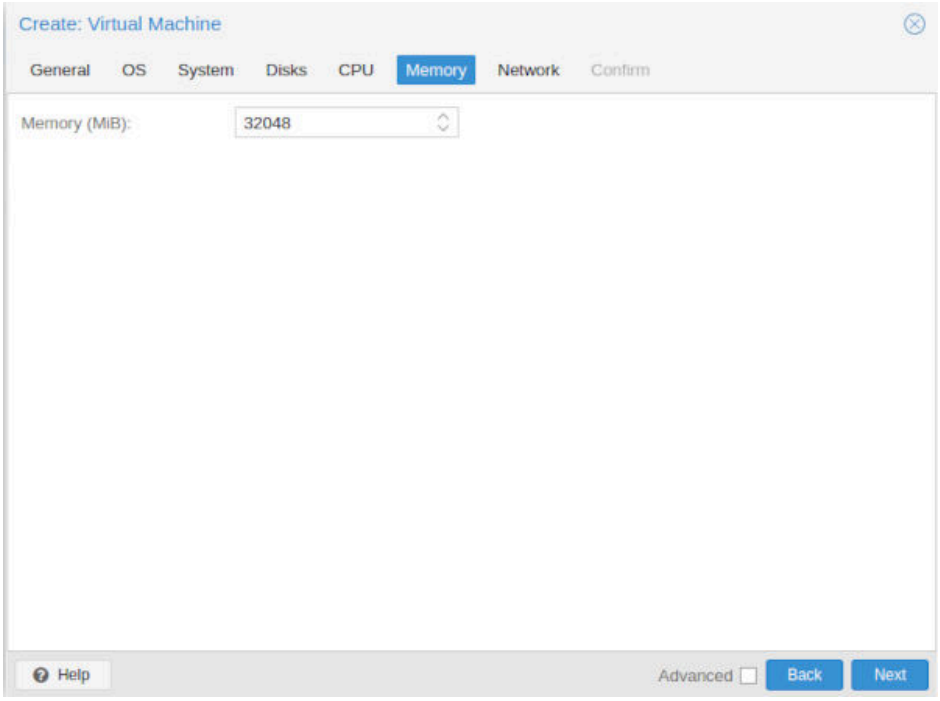


- scsi2 - 10 GB (where the data will be stored)

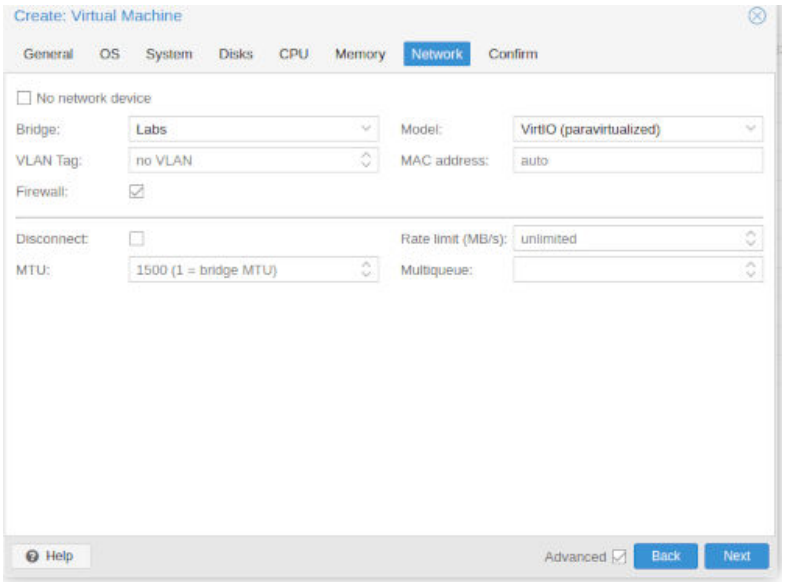


- Configure “CPU” and “Memory” according to your needs.
  - The recommendation is a minimum of 4 cores.
  - The recommendation for the Memory is a minimum 32768 MiB.





- Configure “Network” settings (bridge mode, MAC address, etc.).

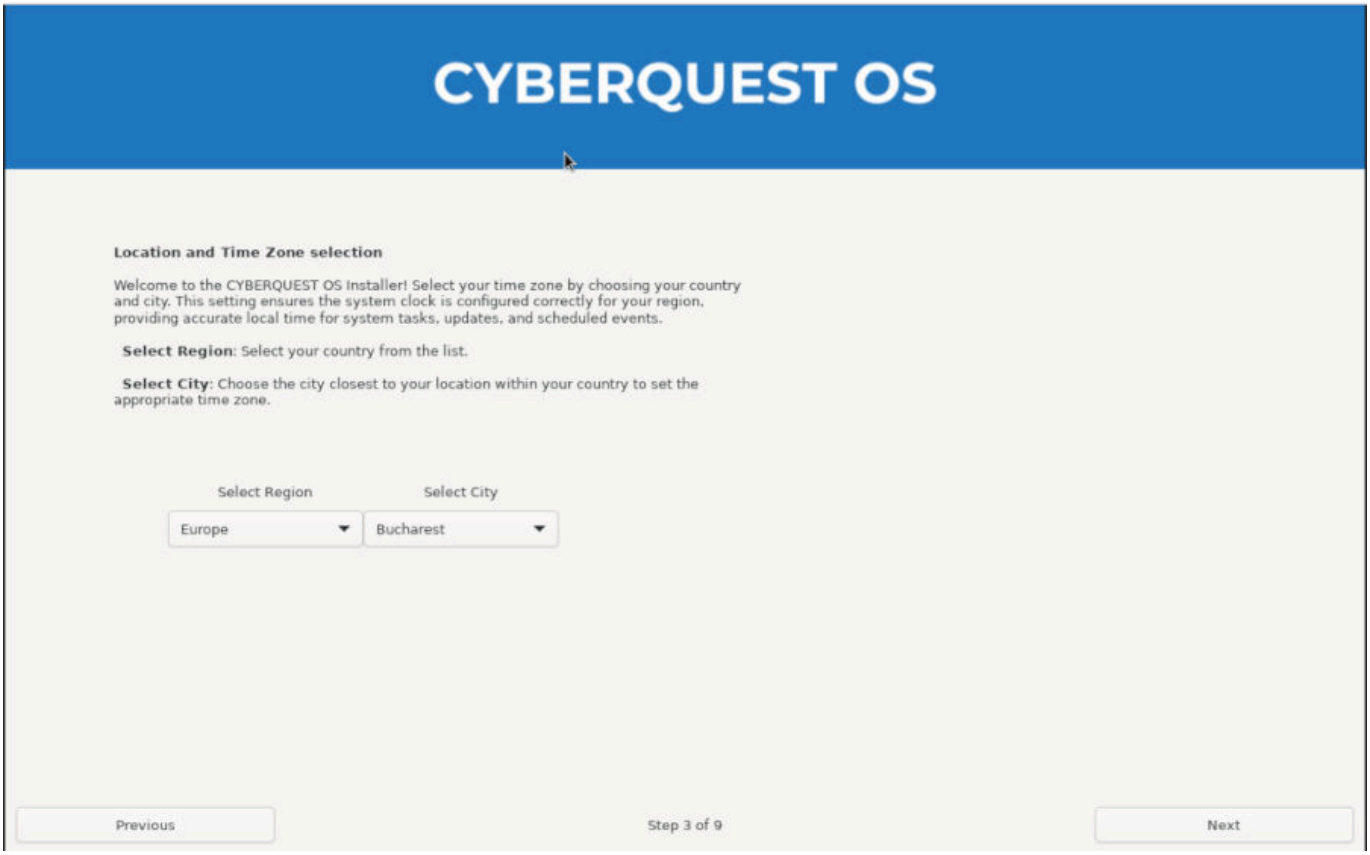


- Review and confirm the settings.

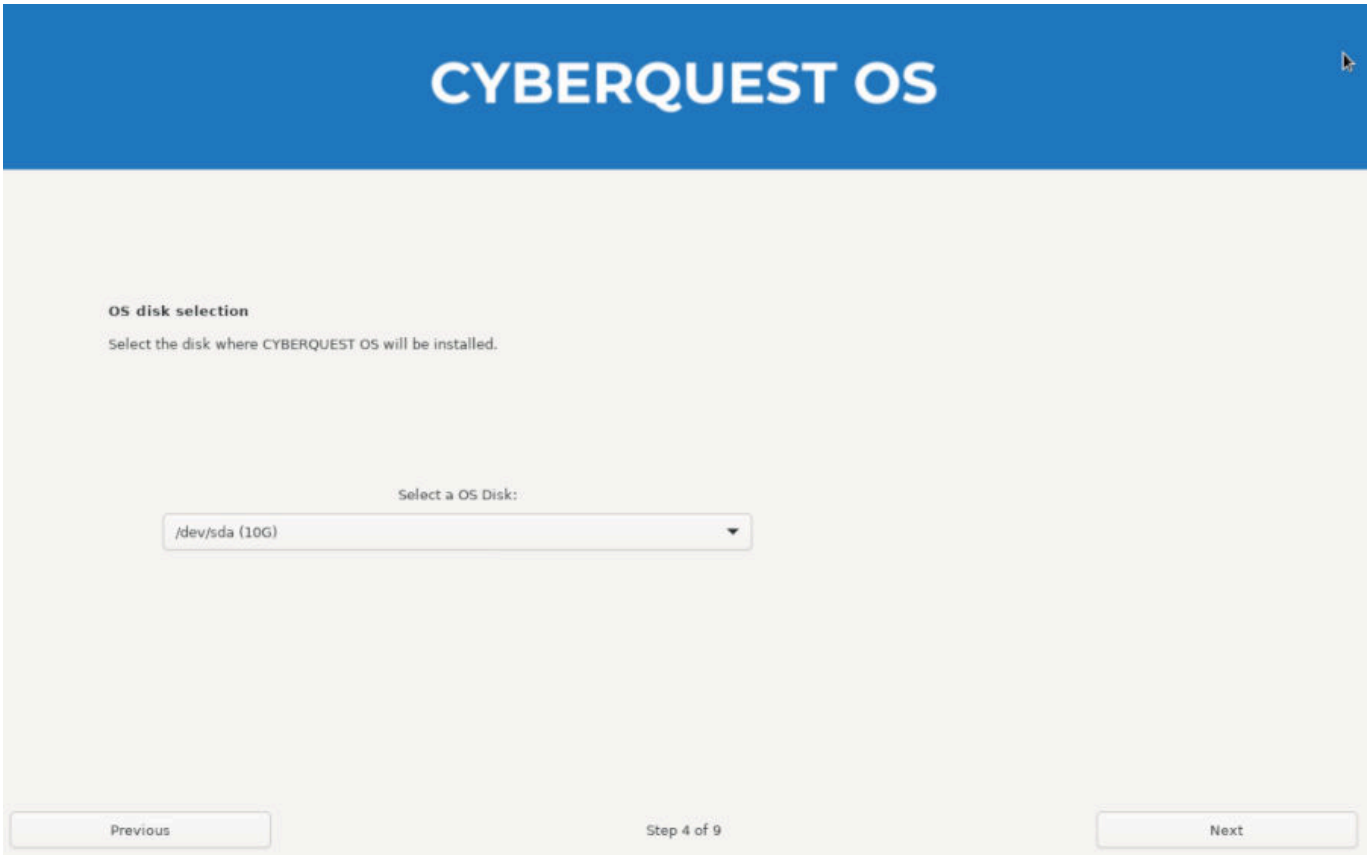
CYBERQUEST OS Installation

Start the newly created VM, select Live System and follow the CYBERQUEST OS Installation steps.

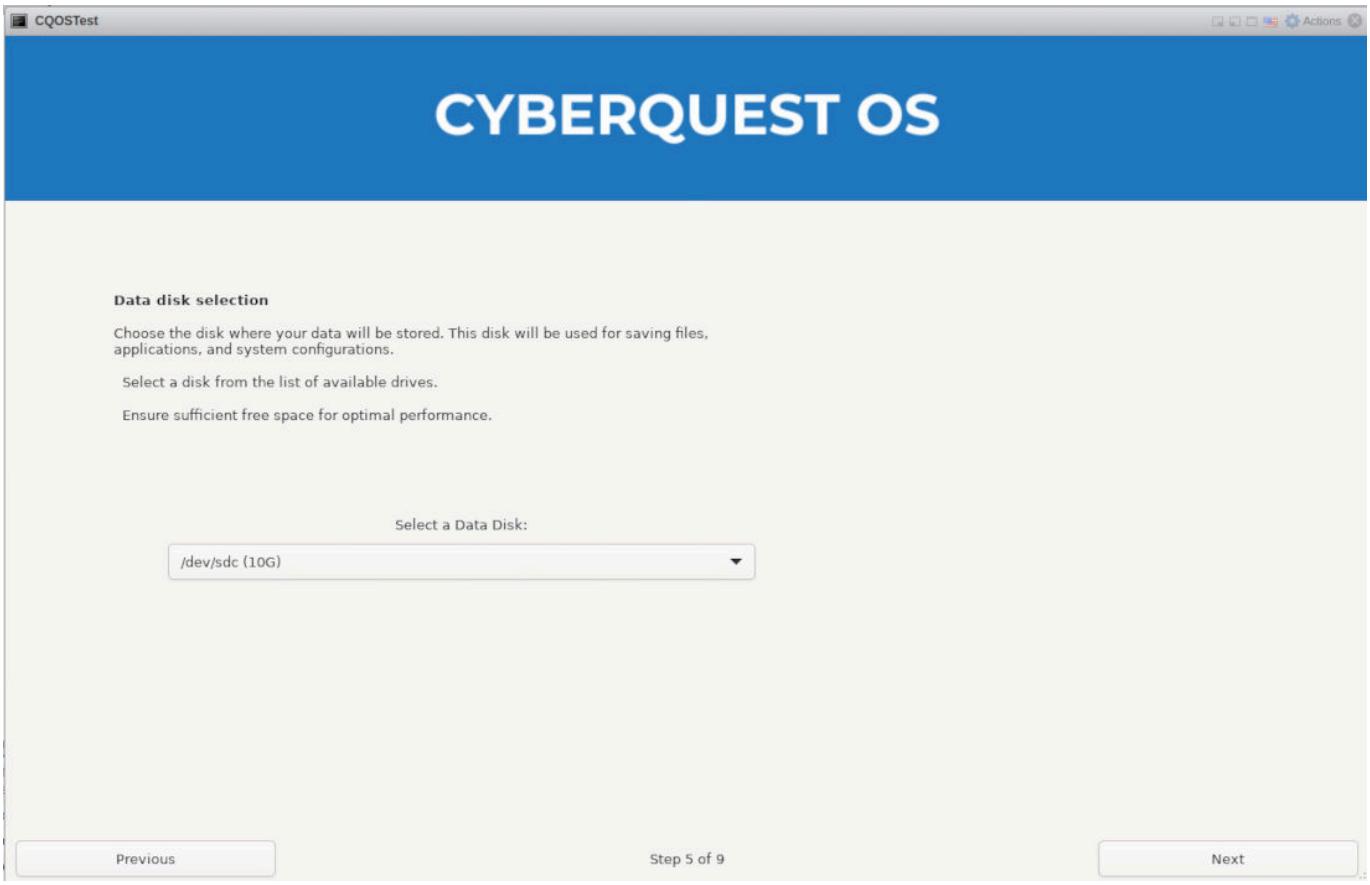
Step 1: Select the Region and City



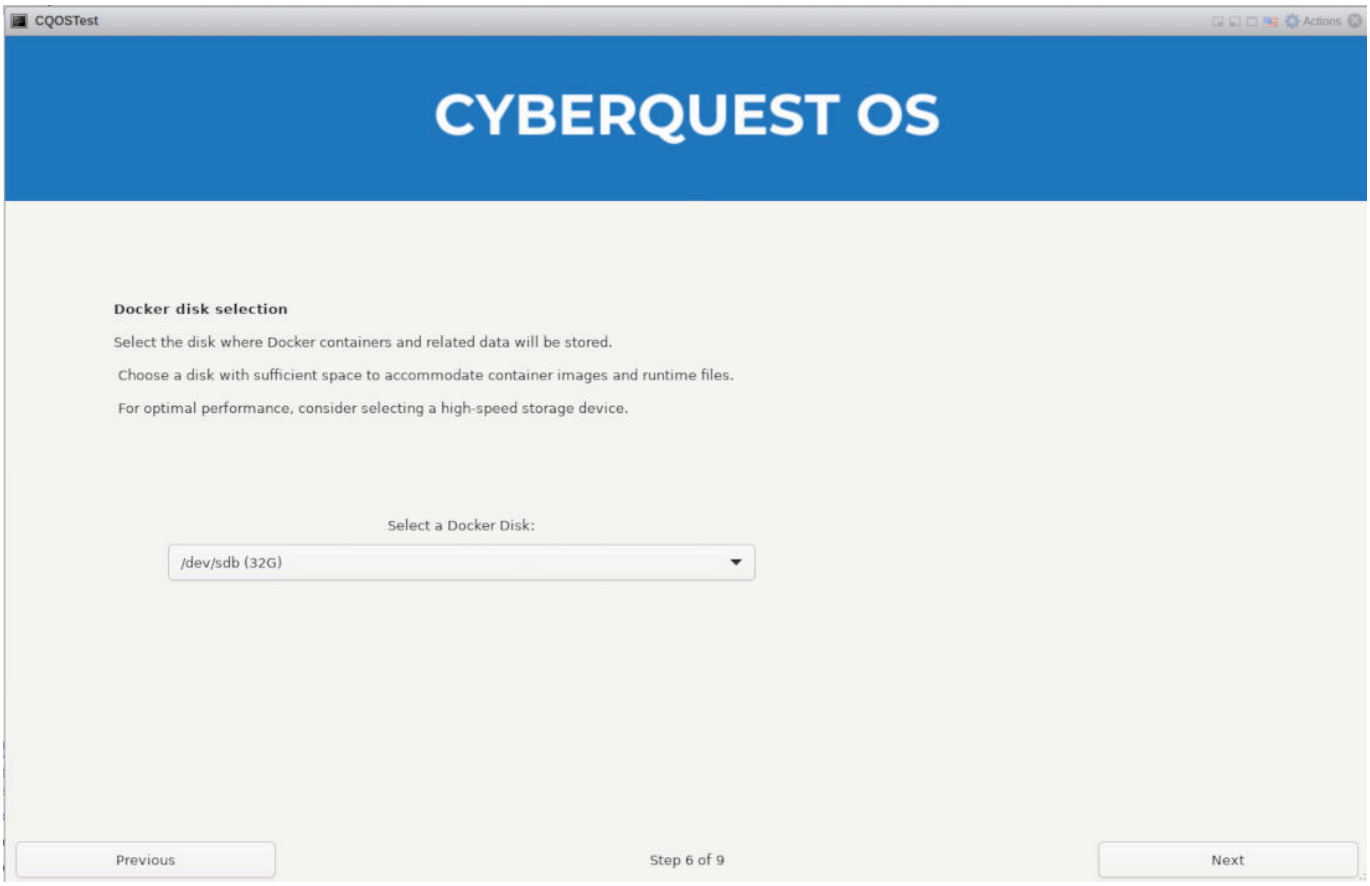
Step 2: Select the disk where the CYBERQUEST OS will be installed.



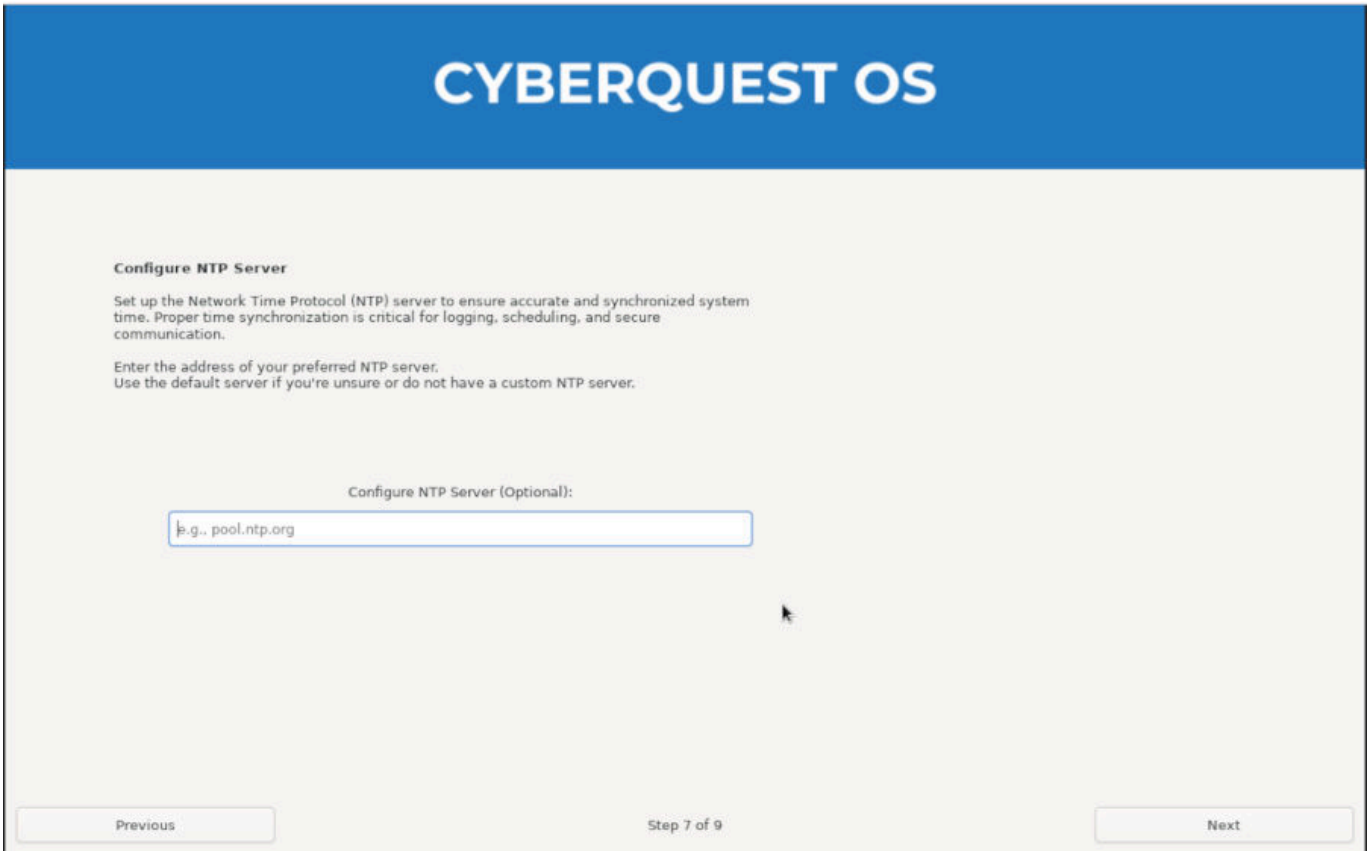
Step 3: Select the disk where the data will be stored.



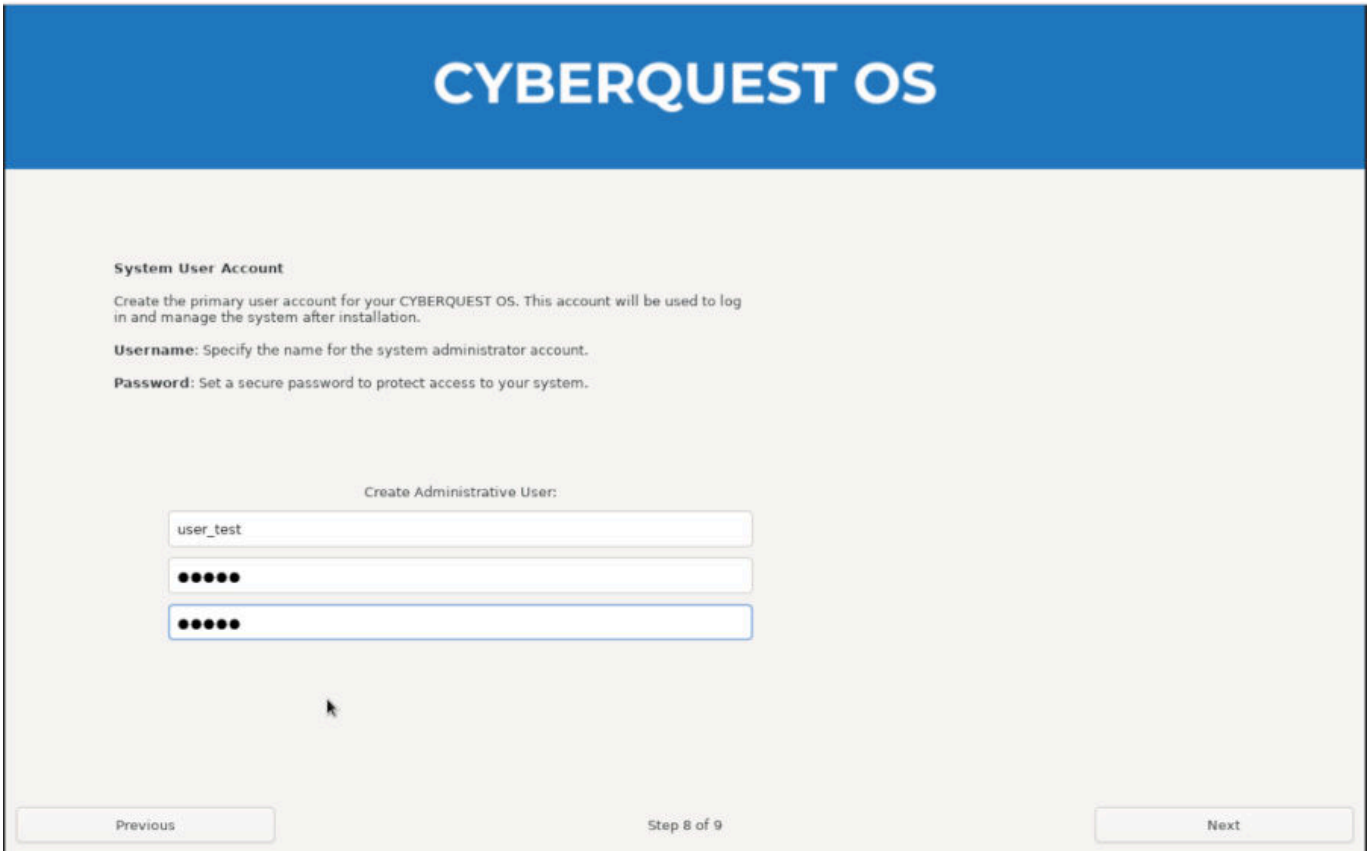
Step 4: Select the disk where Docker containers and realted data will be stored.



Step 5: Set up the Network Time Protocol (NTP) server to ensure accurate and synchronized system time.

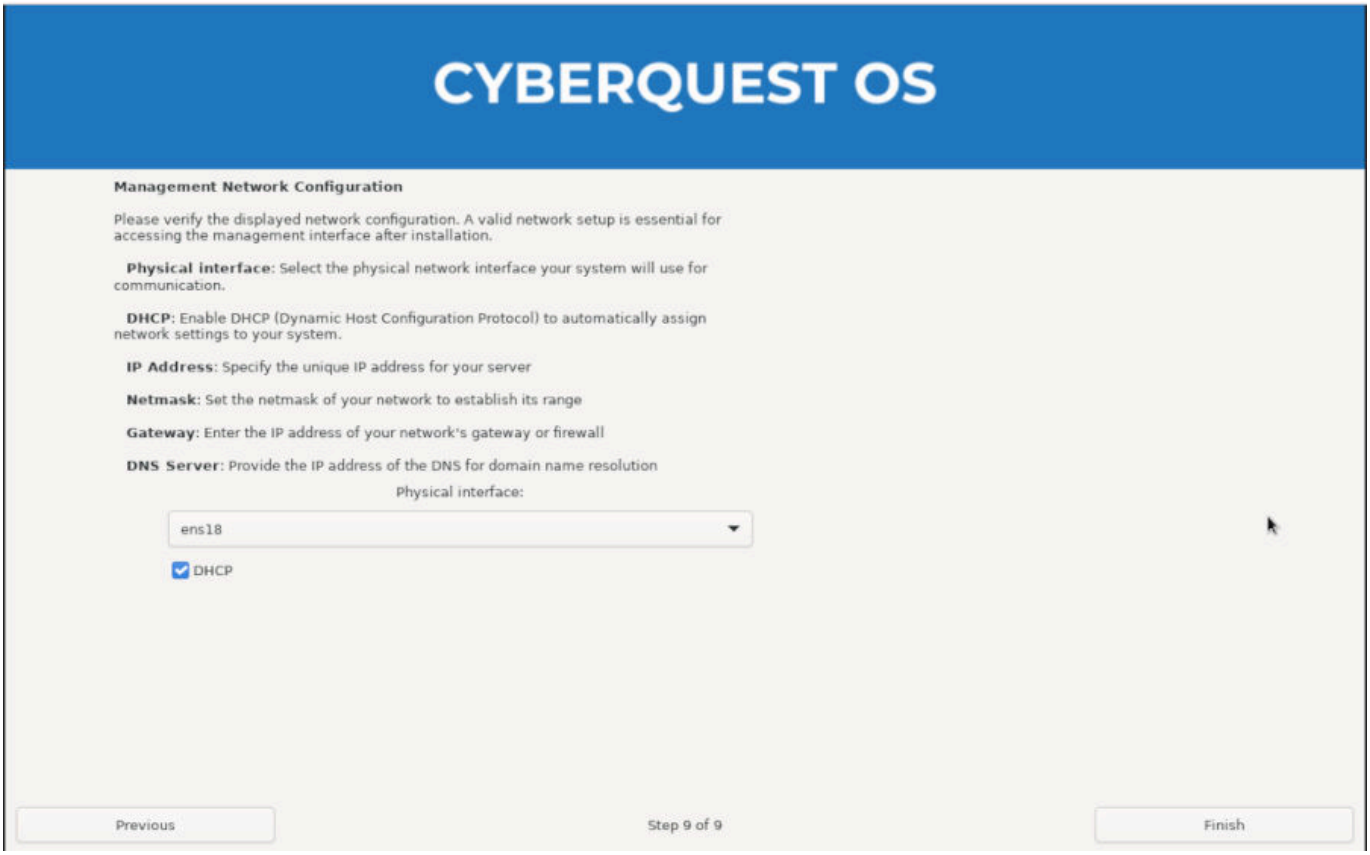


Step 6: Specify the name for the system administrator account and a secure password to protect access to your system.

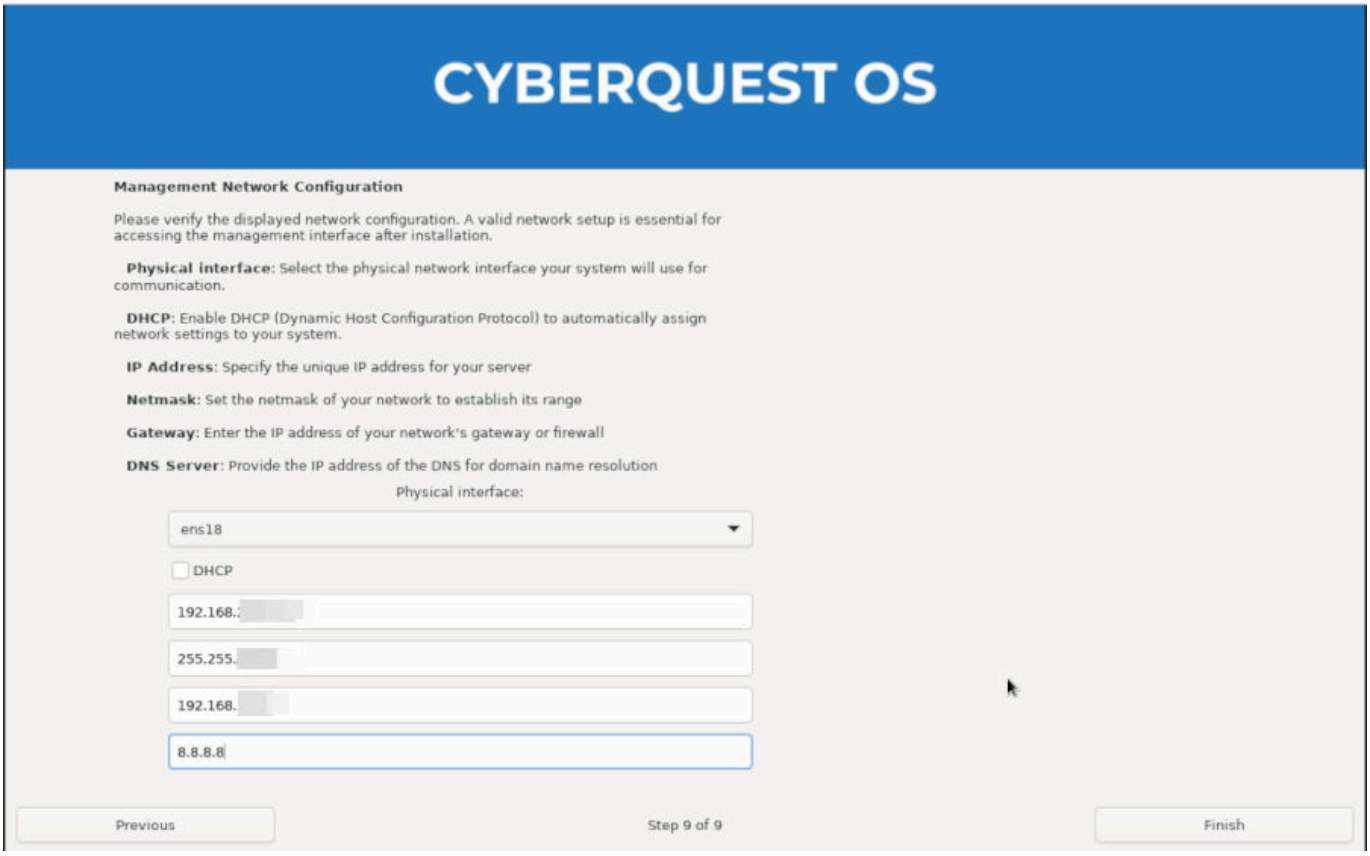


Step 7: Set up the Management Network Configuration using two methods:

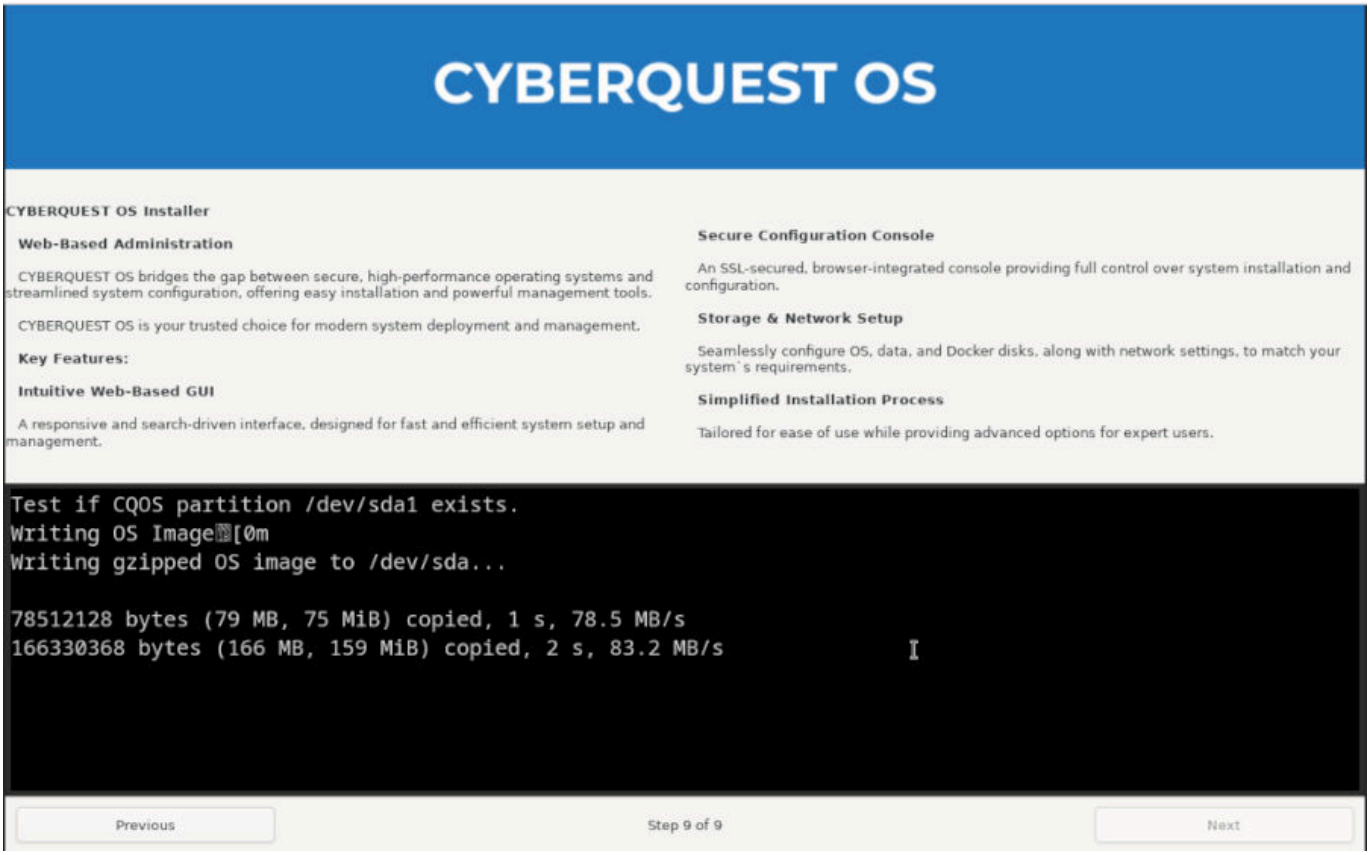
The first method is to use DHCP to automatically assign network settings to the system.

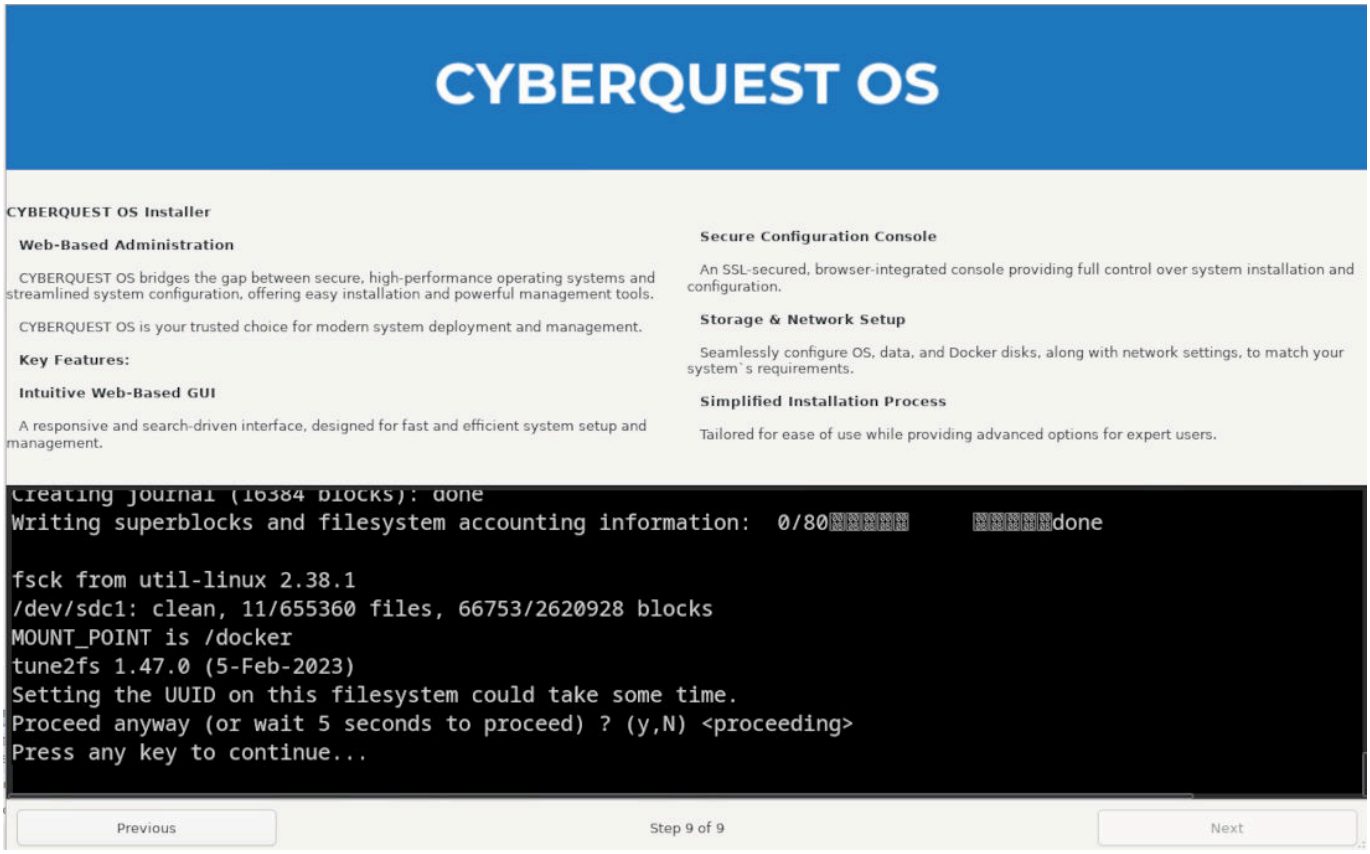


The second method is to manually configure the IP Address, Netmask, Gateway, and DNS Server.



- Click **Finish** and follow the installation prompts. Scroll down to proceed with the installation. Once it's complete, press any key to restart the machine.

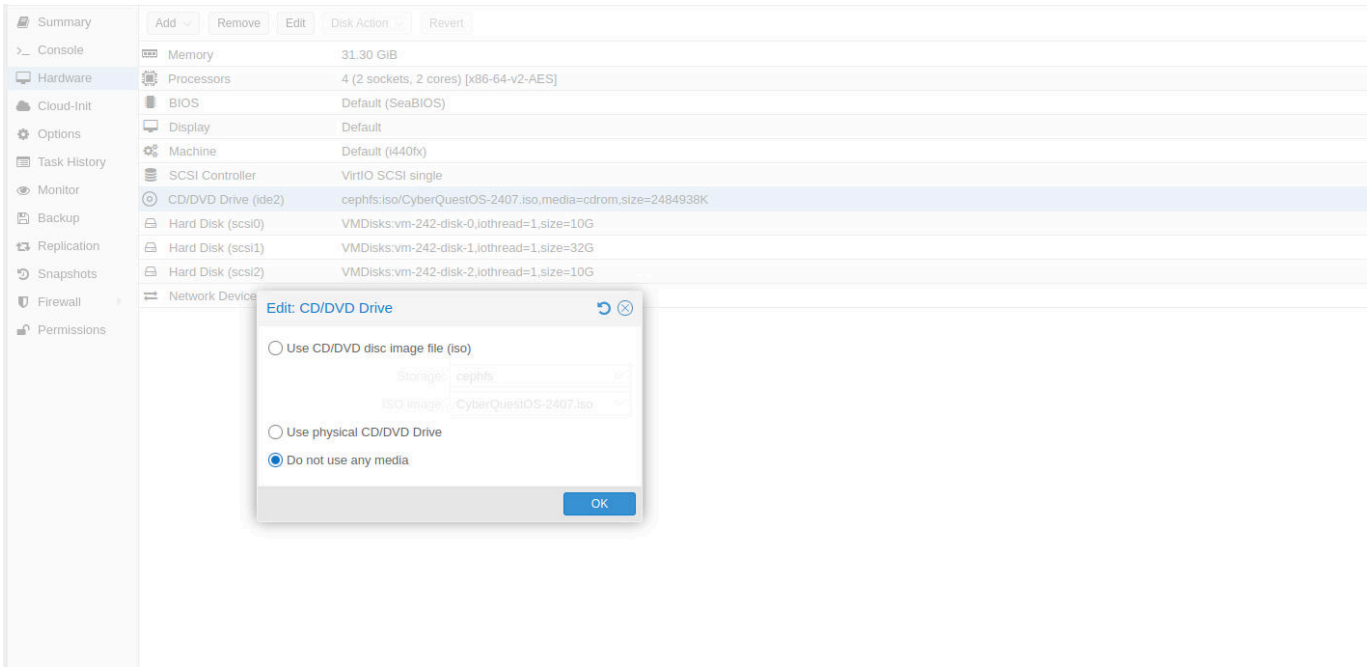


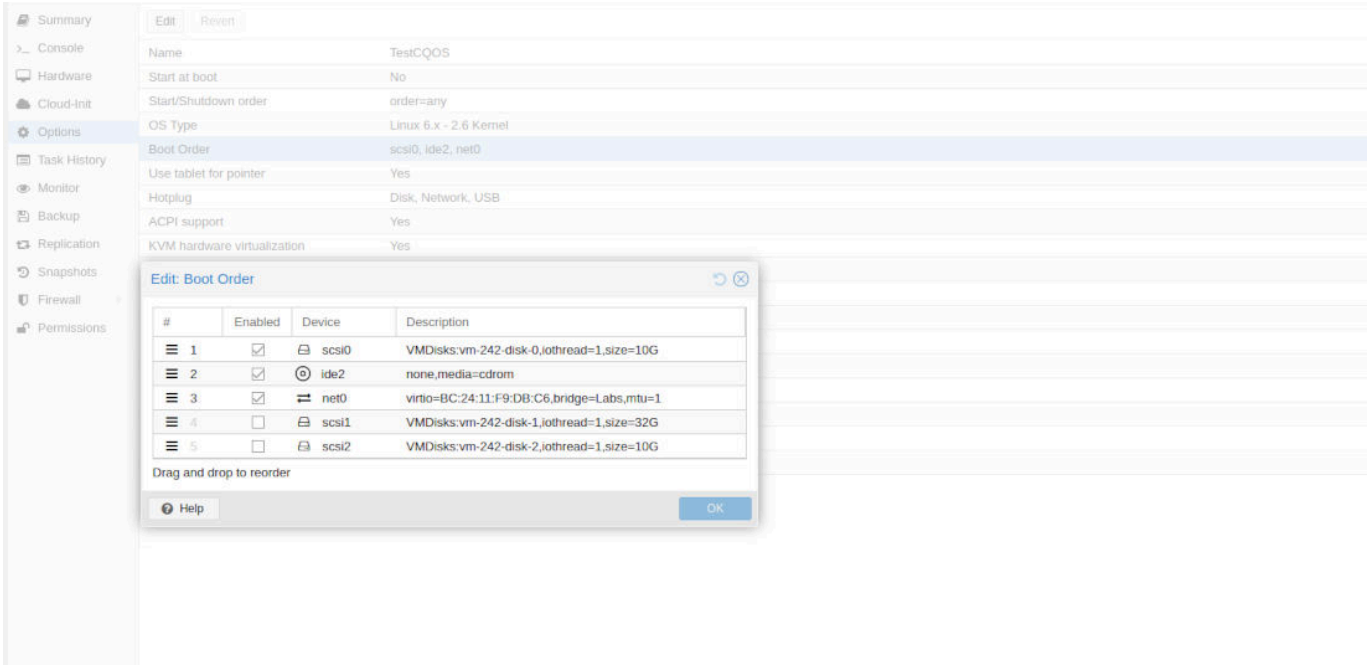


After the restart, the CD will be removed, and the boot order in PROXMOX should be verified to ensure the partition where the OS was installed (e.g., scsi0) is set as the first boot device.

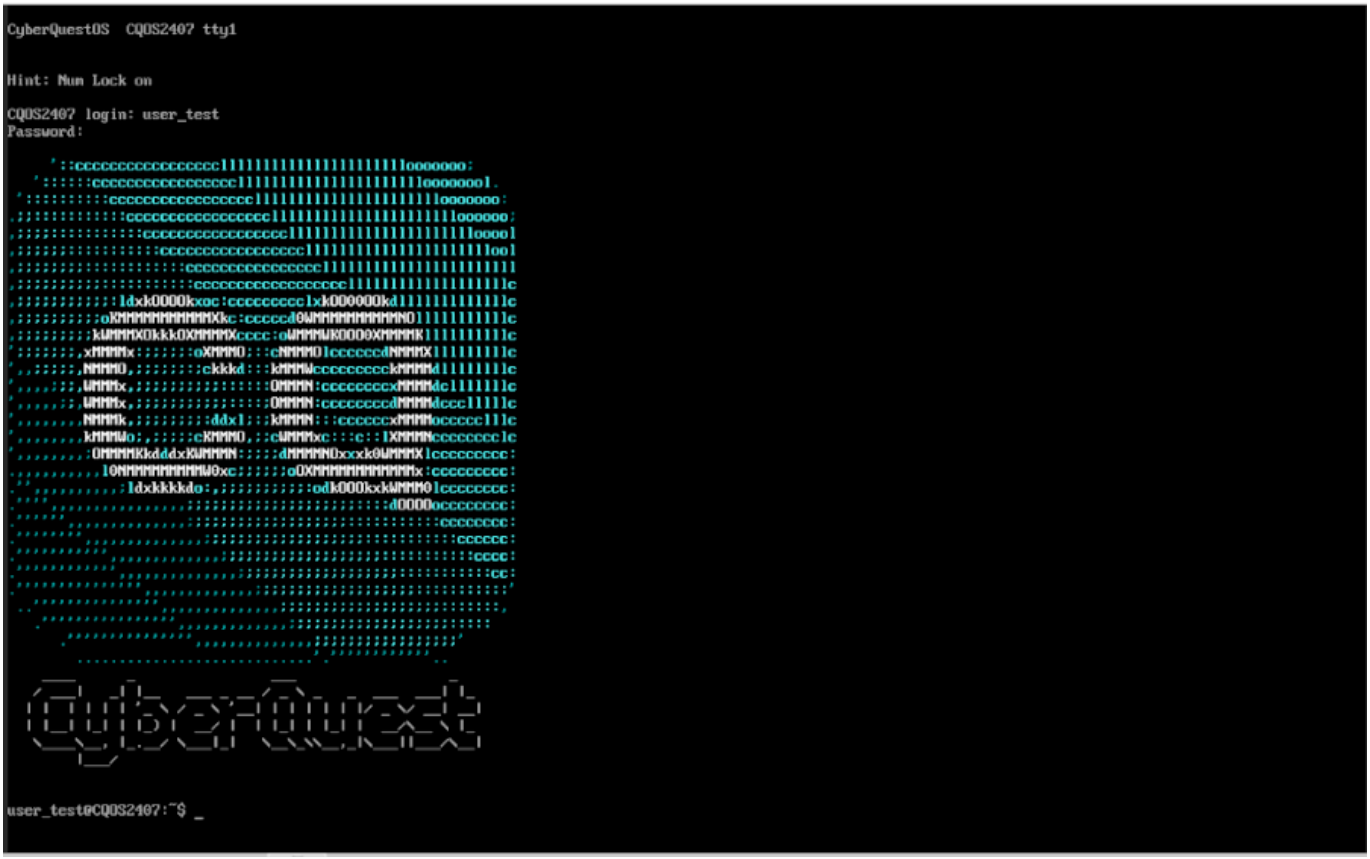
```
[  OK  ] Unmounted run-live-overlay.mount - /run/live/overlay.
[  OK  ] Unmounted run-live-rootfs-filesystem.squashfs.mount - /run/live/rootfs/filesystem.squashfs.
[  OK  ] Unmounted tmp.mount - /tmp.
[  OK  ] Unmounted usr-lib-live-mount-medium.mount - /usr/lib/live/mount/medium.
[  OK  ] Unmounted usr-lib-live-mount-overlay.mount - /usr/lib/live/mount/overlay.
[  OK  ] Unmounted usr-lib-live-mount-rootfs-filesystem.squashfs.mount - /usr/lib/live/mount/rootfs/filesystem.squashfs.
         Unmounting usr-lib-live-mount.mount - /usr/lib/live/mount...
[  OK  ] Unmounted usr-lib-live-mount.mount - /usr/lib/live/mount.
[  OK  ] Stopped target local-fs-pre.target - Preparation for Local File Systems.
[  OK  ] Stopped target swap.target - Swaps.
[  OK  ] Reached target umount.target - Unmount All Filesystems.
[  OK  ] Stopped systemd-tmpfiles-setup-dev.service - Create Static Device Nodes in /dev.
[  OK  ] Stopped systemd-sysusers.service - Create System Users.
[  OK  ] Stopped systemd-remount-fs.service - Remount Root and Kernel File Systems.
[  OK  ] Reached target shutdown.target - System Shutdown.
[  OK  ] Reached target final.target - Late Shutdown Services.
[  OK  ] Finished systemd-reboot.service - System Reboot.
[  OK  ] Reached target reboot.target - System Reboot.
[  316.990586] systemd-shutdown[1]: Syncing filesystems and block devices.
[  316.992028] systemd-shutdown[1]: Sending SIGTERM to remaining processes...
[  316.998837] systemd-journald[469]: Received SIGTERM from PID 1 (systemd-shutdow).
[  317.015764] systemd-shutdown[1]: Sending SIGKILL to remaining processes...
[  317.021828] systemd-shutdown[1]: Unmounting file systems.
[  317.024363] (sd-remount)[1155]: Remounting '/' read-only with options 'lowerdir=/run/live/rootfs/filesystem.squashfs/,upperdir=/run/live/overlay/rw,workdir=/
run/live/overlay/work,redirect_dir=on'.
[  317.045006] (sd-umount)[1156]: Unmounting '/run/live/medium'.
[  317.046353] (sd-umount)[1156]: Failed to unmount /run/live/medium: Device or resource busy
[  317.047509] systemd-shutdown[1]: Not all file systems unmounted, 1 left.
[  317.048550] systemd-shutdown[1]: Deactivating swaps.
[  317.050154] systemd-shutdown[1]: All swaps deactivated.
[  317.051505] systemd-shutdown[1]: Detaching loop devices.
[  317.053840] systemd-shutdown[1]: Detaching loopback /dev/loop0.
[  317.054582] systemd-shutdown[1]: Could not detach loopback /dev/loop0: Device or resource busy
[  317.055132] systemd-shutdown[1]: Not all loop devices detached, 1 left.
[  317.055608] systemd-shutdown[1]: Stopping MD devices.
[  317.056086] systemd-shutdown[1]: All MD devices stopped.
[  317.056491] systemd-shutdown[1]: Detaching DM devices.
[  317.056979] systemd-shutdown[1]: All DM devices detached.
[  317.057522] systemd-shutdown[1]: Unmounting file systems.
[  317.058675] (sd-umount)[1158]: Unmounting '/run/live/medium'.
[  317.059072] (sd-umount)[1158]: Failed to unmount /run/live/medium: Device or resource busy
[  317.061970] systemd-shutdown[1]: Not all file systems unmounted, 1 left.
[  317.062818] systemd-shutdown[1]: Detaching loop devices.
[  317.064392] systemd-shutdown[1]: Detaching loopback /dev/loop0.
[  317.065310] systemd-shutdown[1]: Could not detach loopback /dev/loop0: Device or resource busy
[  317.066257] systemd-shutdown[1]: Not all loop devices detached, 1 left.
[  317.066843] systemd-shutdown[1]: Cannot finalize remaining file systems, loop devices, continuing.


Please remove the live-medium, close the tray (if any) and press ENTER to continue:
```





Once the operating system has booted, the user can log in using the credentials created during the installation process above.



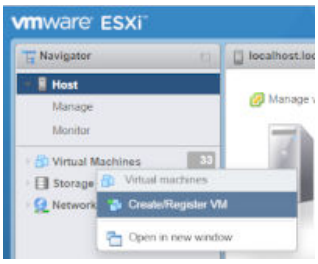
VMware Installation

Log in to the VMware Web Interface

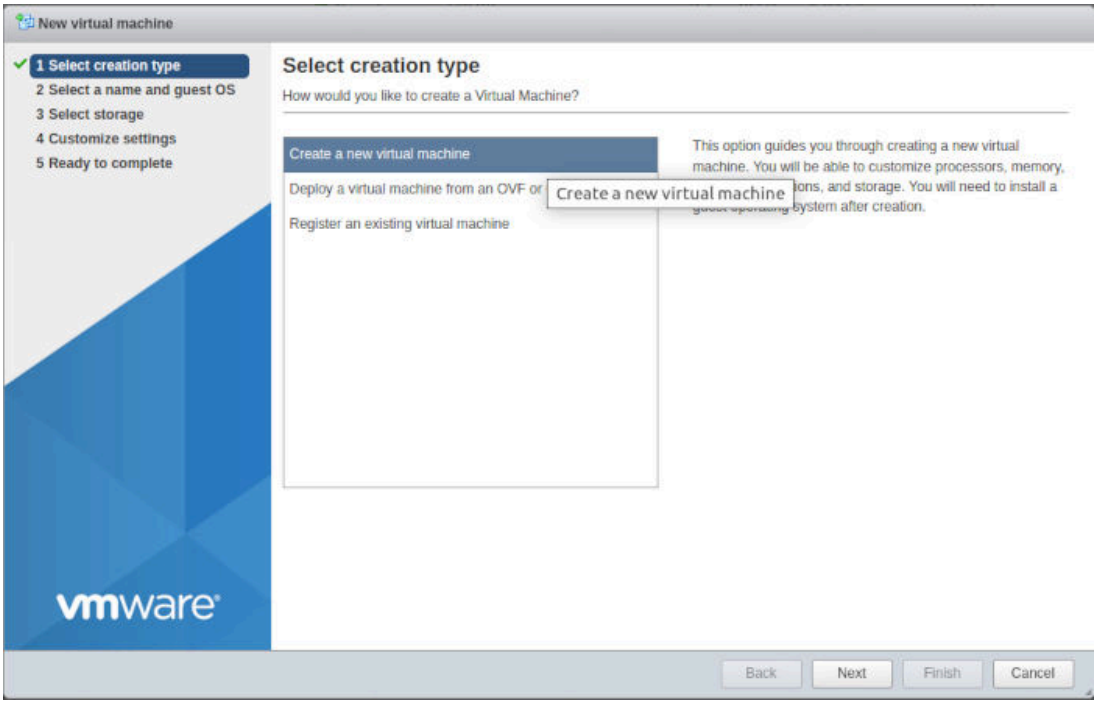
Log in to the VMware Web Interface: Use the credentials set during installation.

Create a New VM

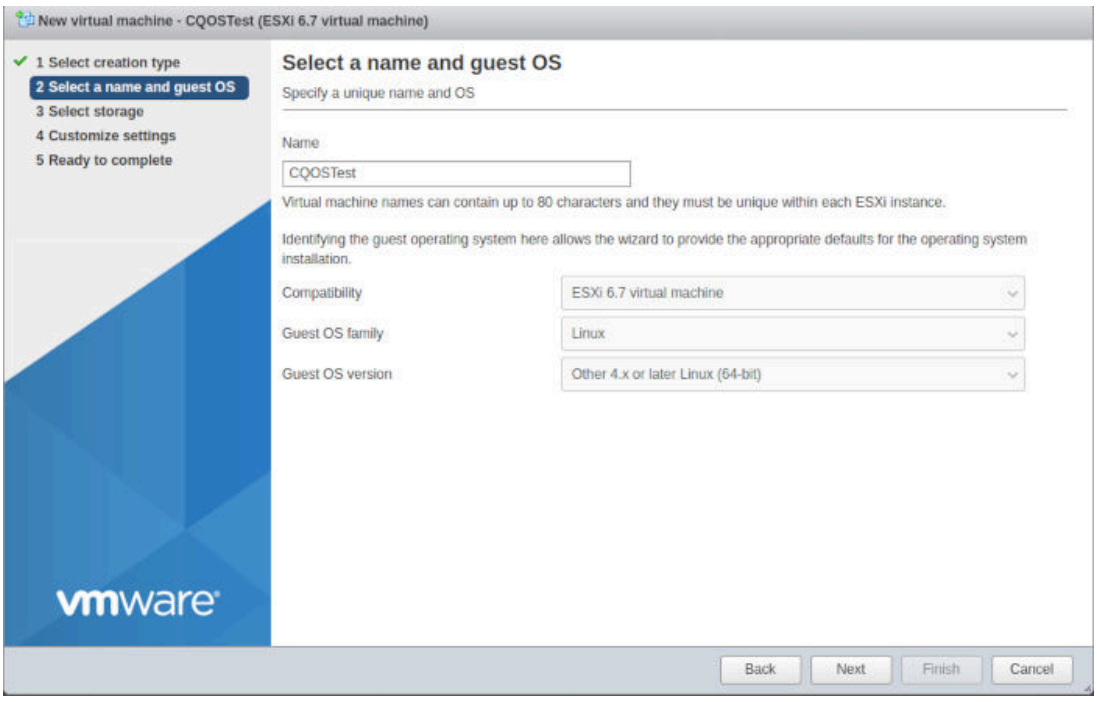
1.Right click on **Virtual Machines** and select **Create/Register VM**.



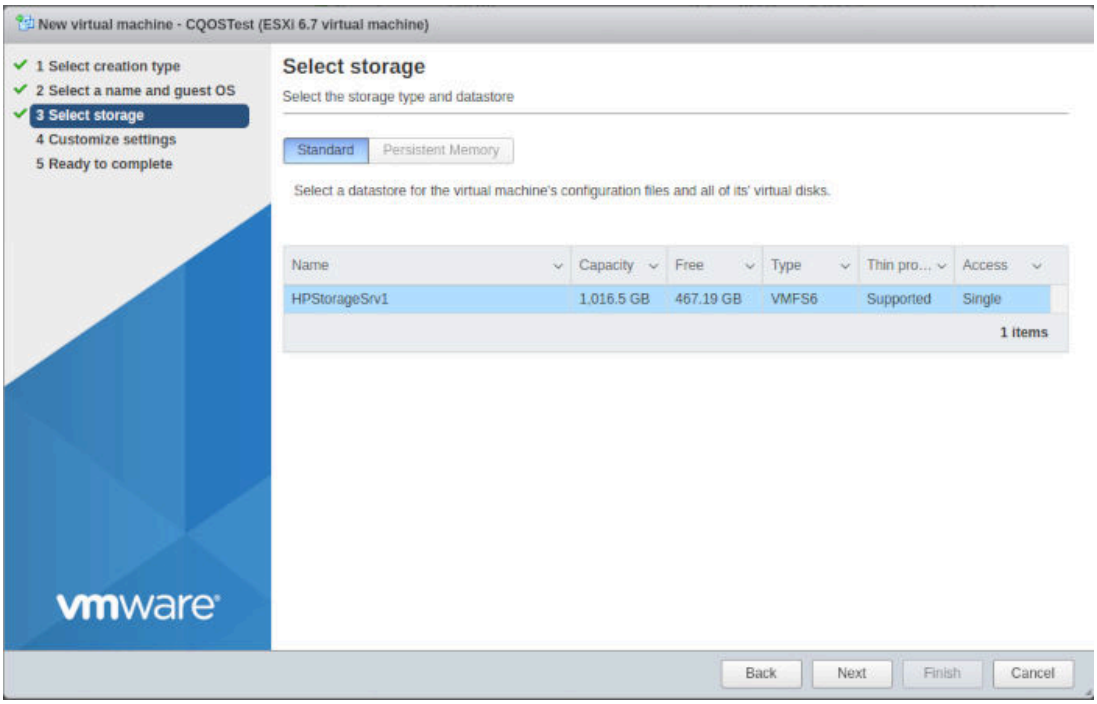
2.Select Create a new virtual machine and click **Next**.



3.Choose a **name** for the virtual machine ("CQOSTest" in this example), select **Guest OS familiy** ("Linux" in this example) and choose **Guest OS version** ("Debian GNU/Linux 10 (64-bit)") and click **Next**.

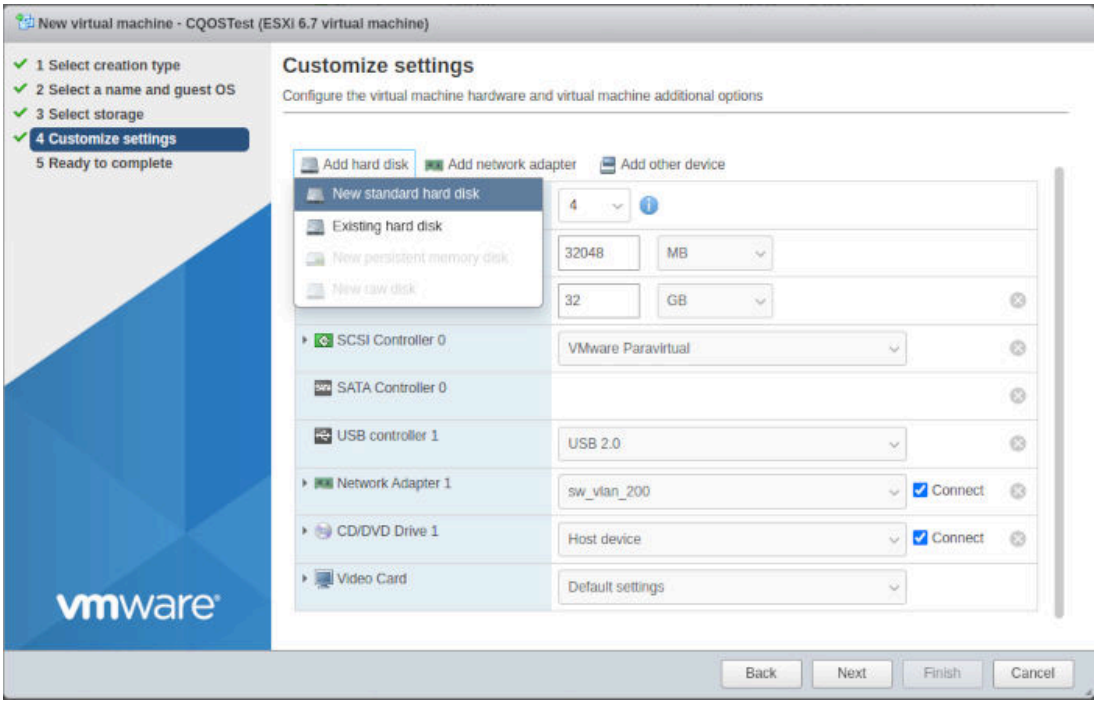


4.Choose the storage where to import the virtual machine and click **Next**.



5.Customize settings - configure the virtual machine hardware and additional options.

- Configure "CPU" and "Memory" according to your needs.
  - The recommendation is a minimum of 4 cores.
  - The recommendation for the Memory is a minimum 32048 MiB.
- Configure three disk partitions. To add more disk partitions click on ***Add hard disk*** and choose ***New standard hard disk***.

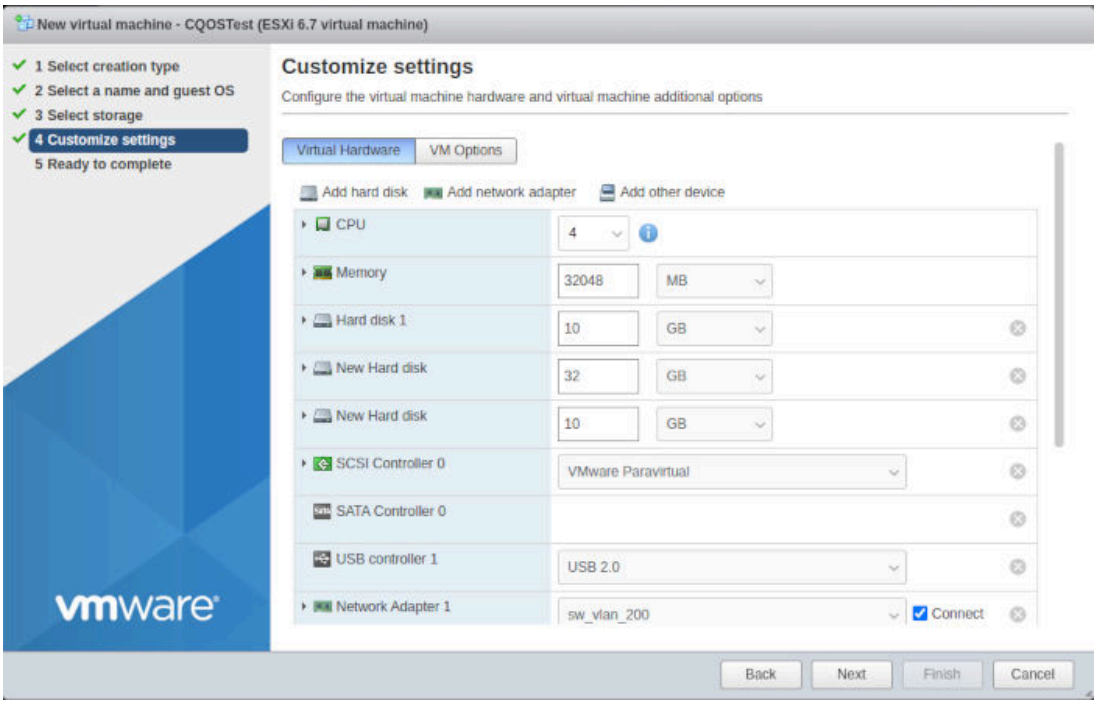


The recommended setup is:

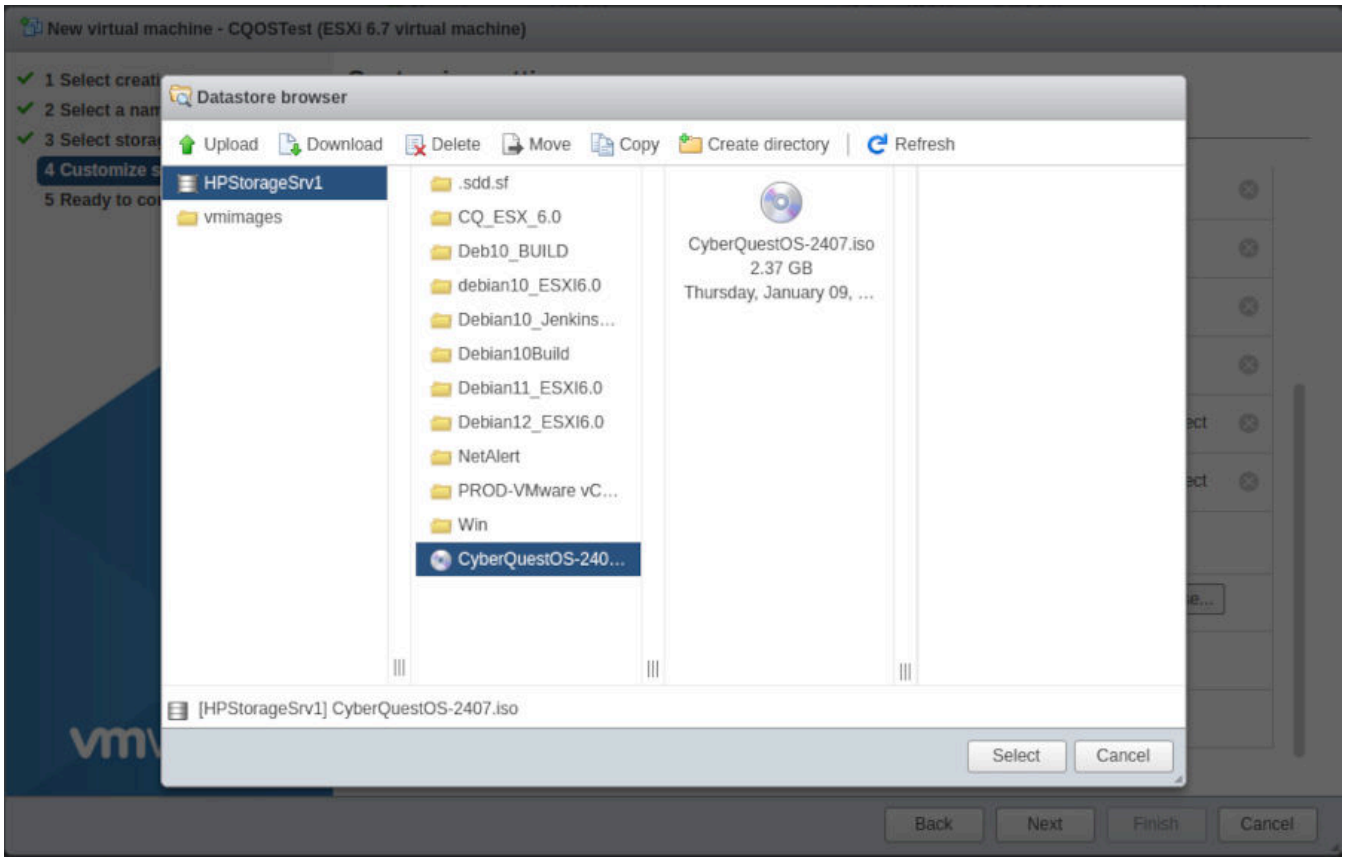
Hard disk 1 - 10 GB (where the Operating System will be installed)

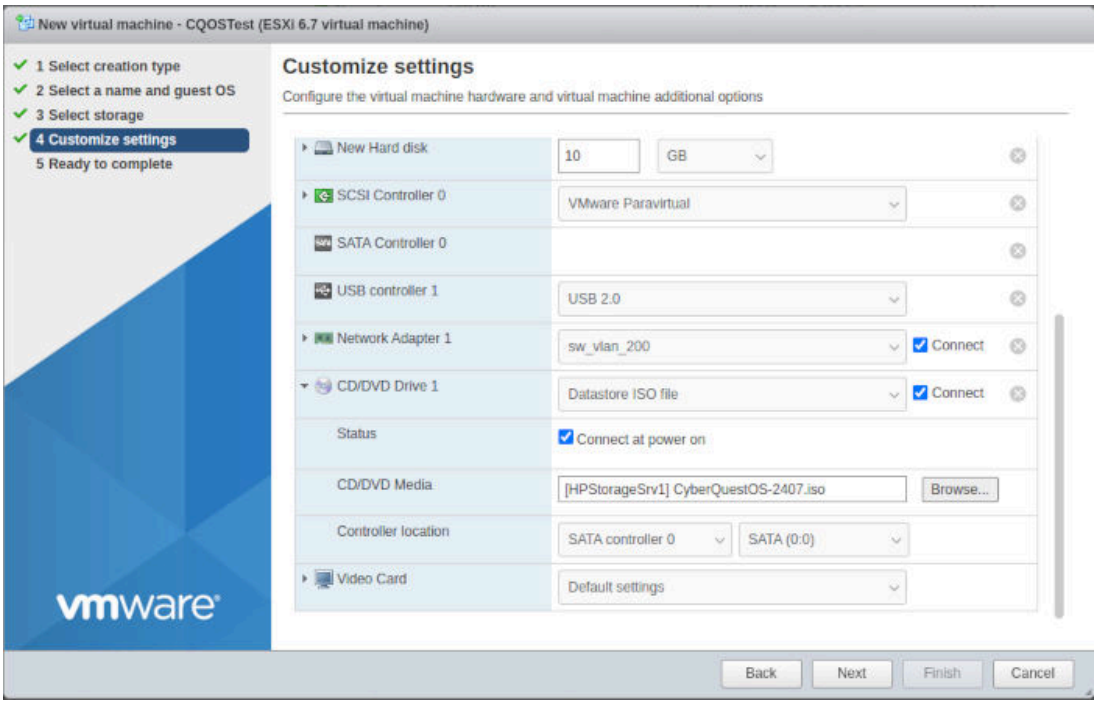
New Hard disk - 32 GB (where the Docker containers are stored)

New Hard disk - 10 GB (where the data will be stored)



- Configure “Network” settings.
- Go to CD/DVD Drive 1 choosing Datastore ISO file and select the CyberQuestOS-2407.iso.



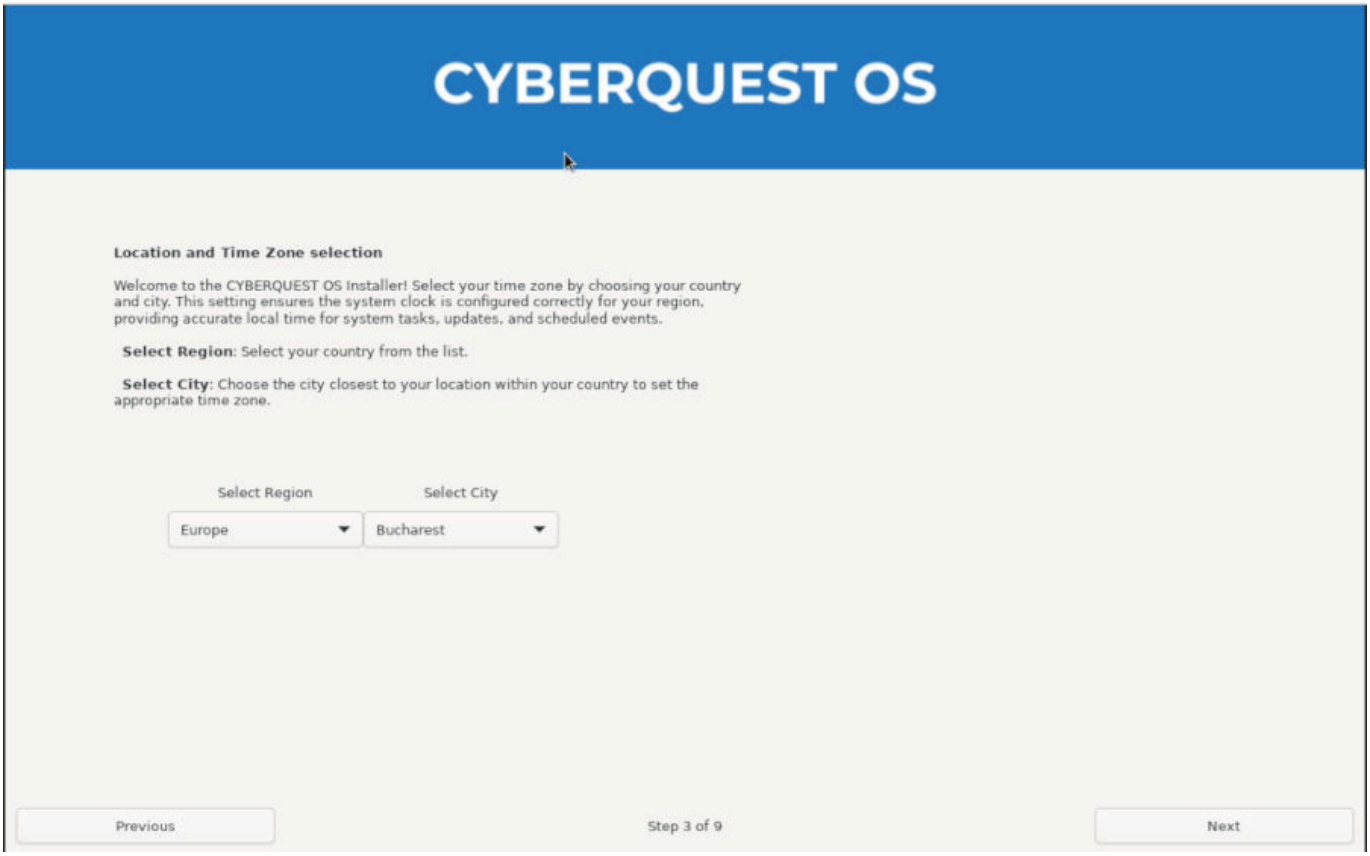


6.Review and confirm the settings.

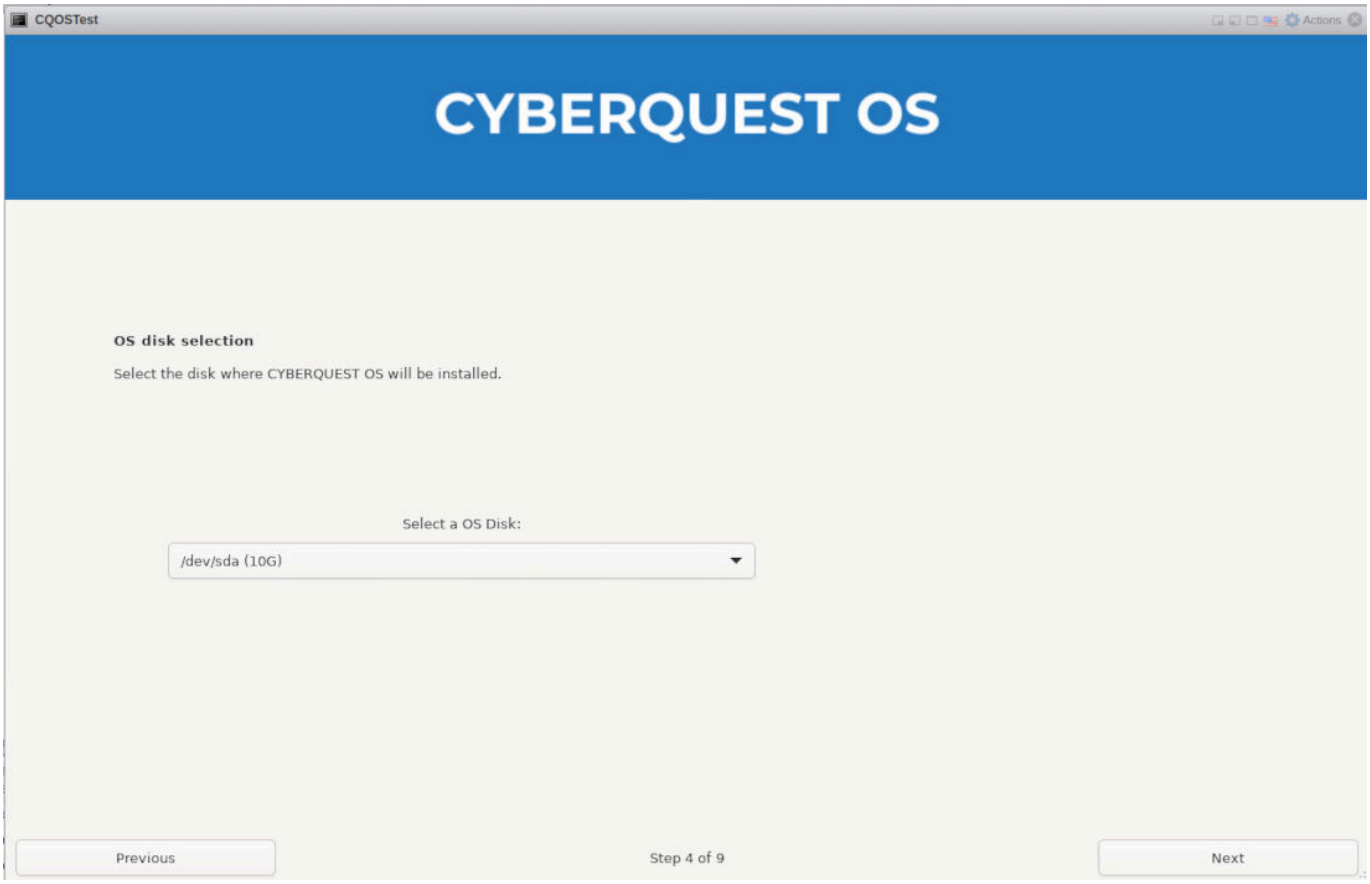
CYBERQUEST OS Installation

Start the newly created VM, select Live System and follow the CYBERQUEST OS Installation steps.

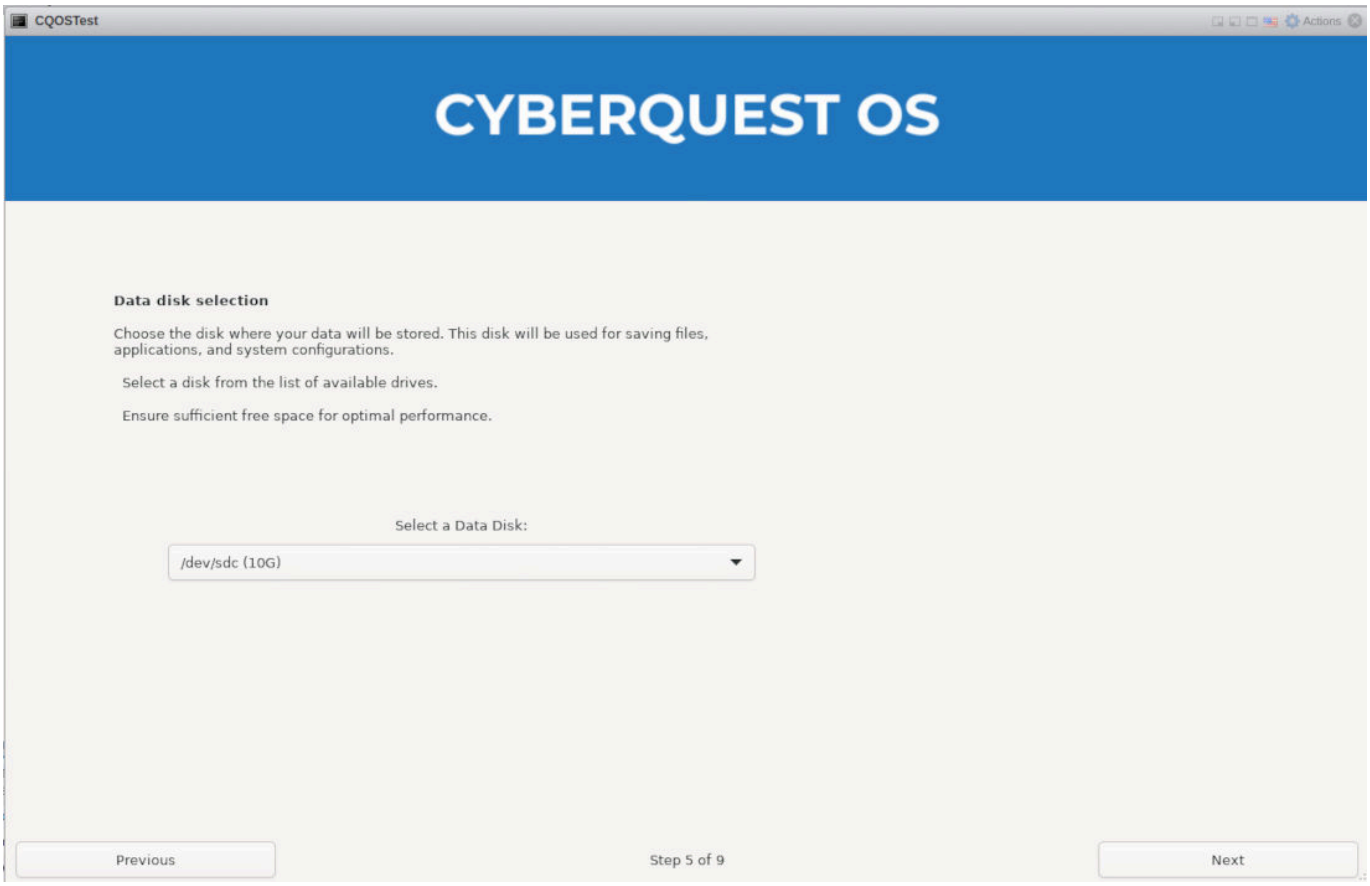
Step 1: Select the Region and City



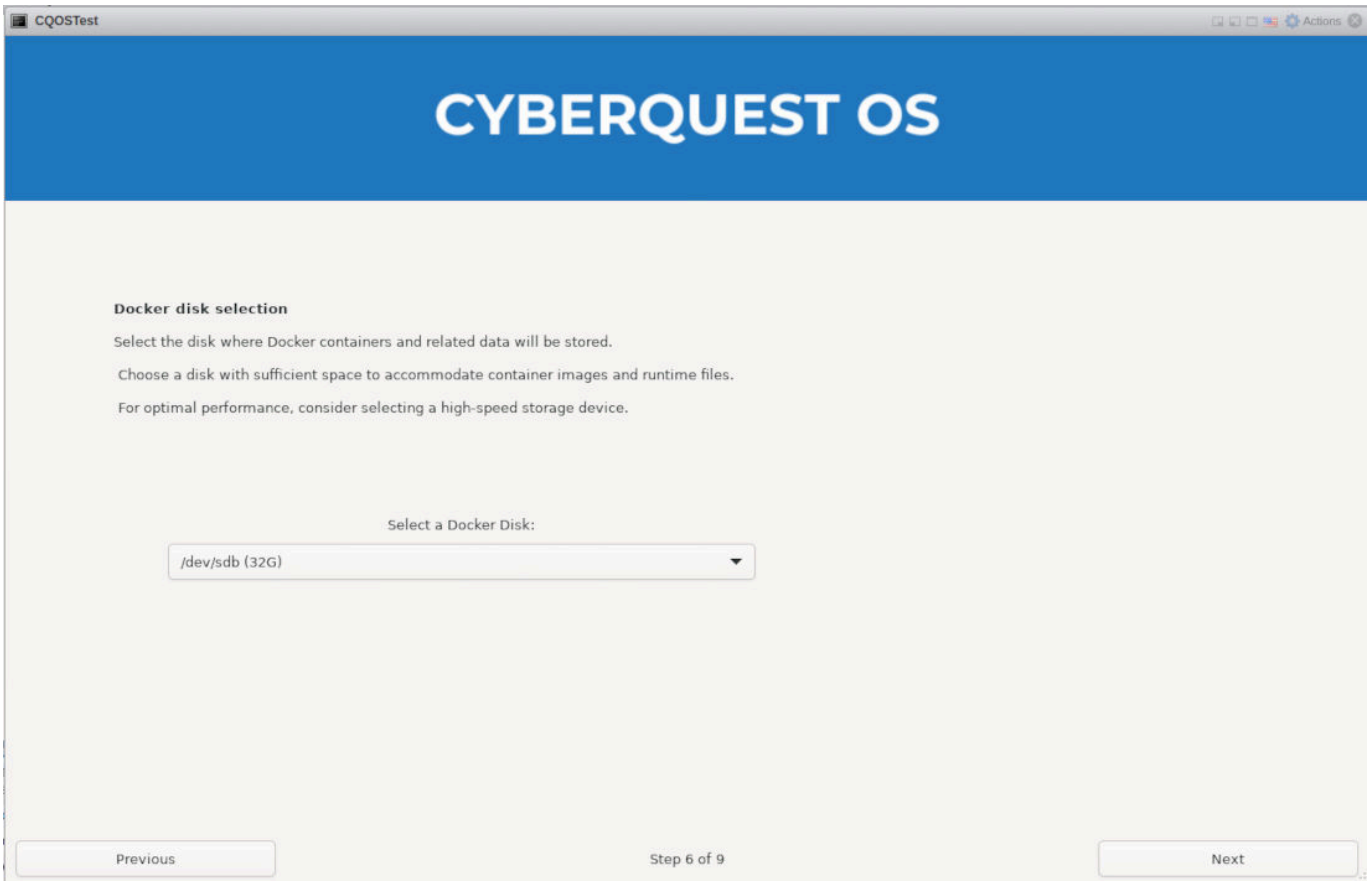
Step 2: Select the disk where the CYBERQUEST OS will be installed.



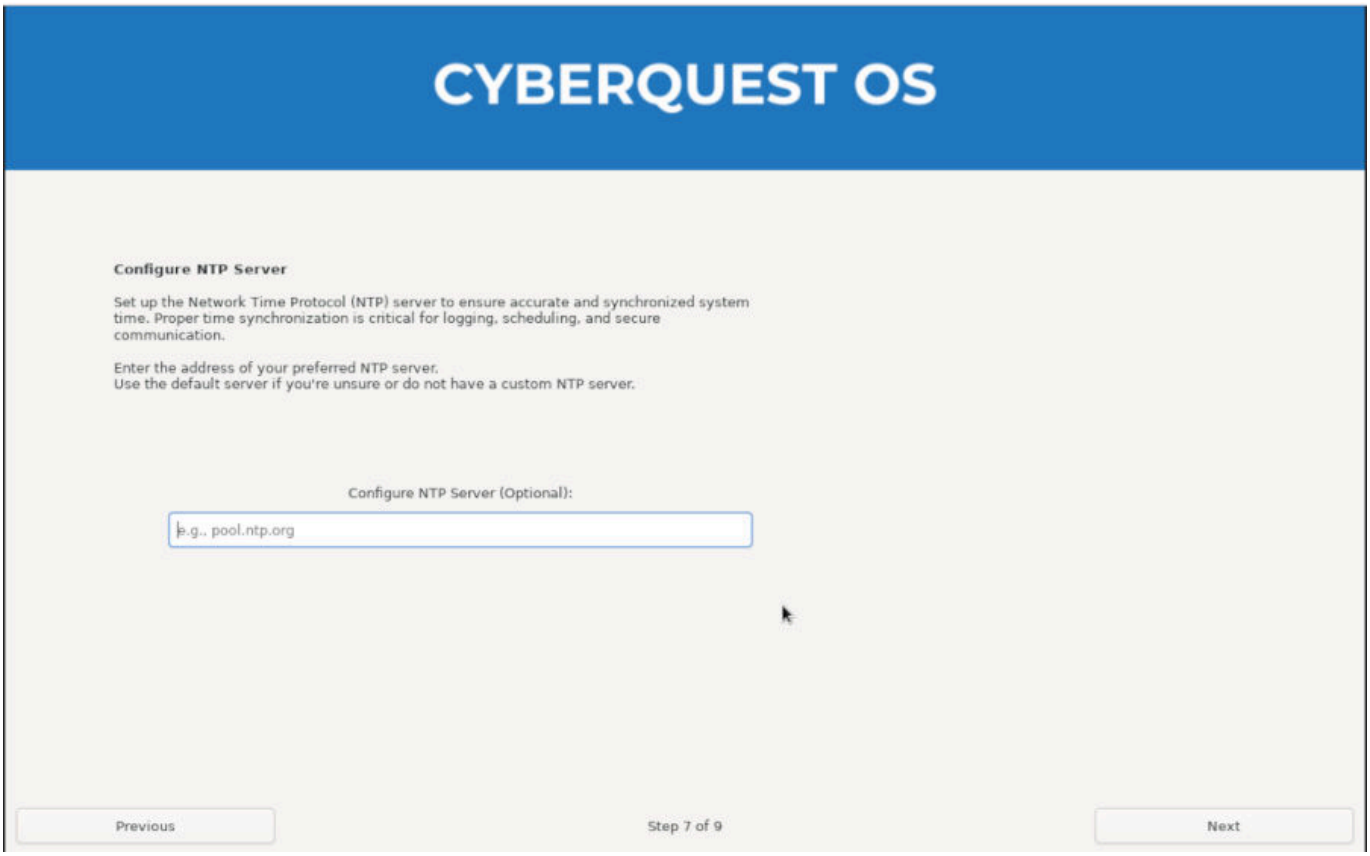
Step 3: Select the disk where the data will be stored.



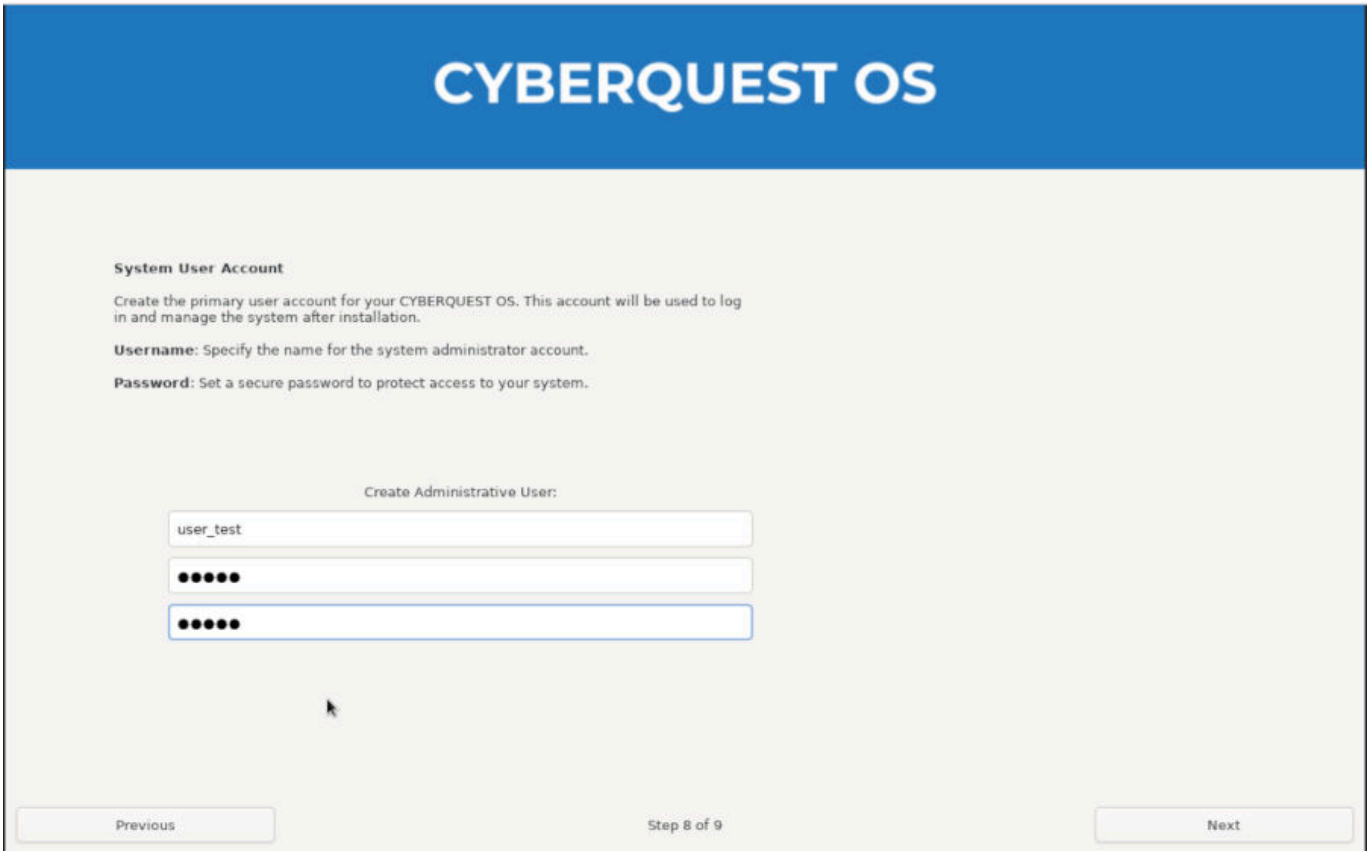
Step 4: Select the disk where Docker containers and related data will be stored.



Step 5: Set up the Network Time Protocol (NTP) server to ensure accurate and synchronized system time.

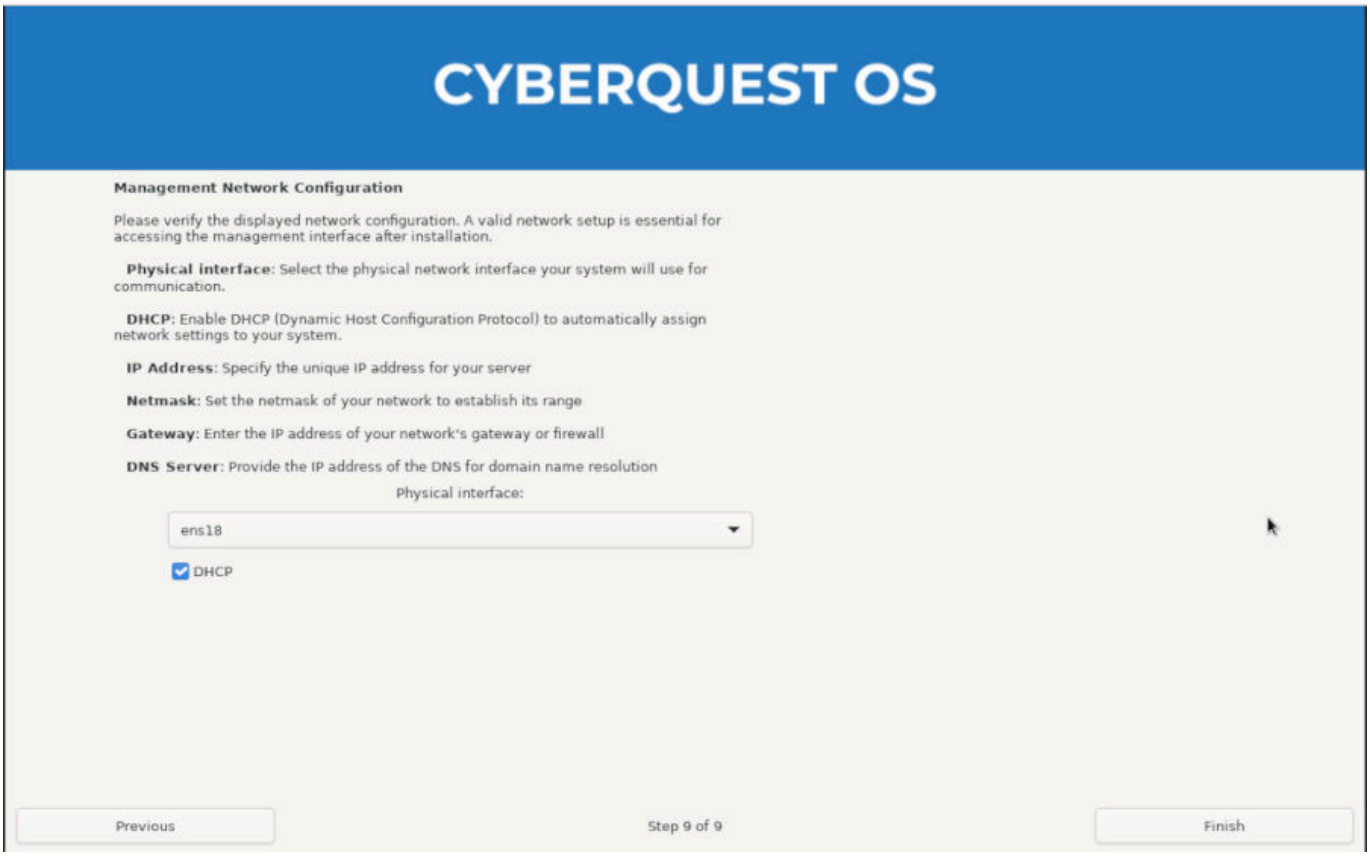


Step 6: Specify the name for the system administrator account and a secure password to protect access to your system.

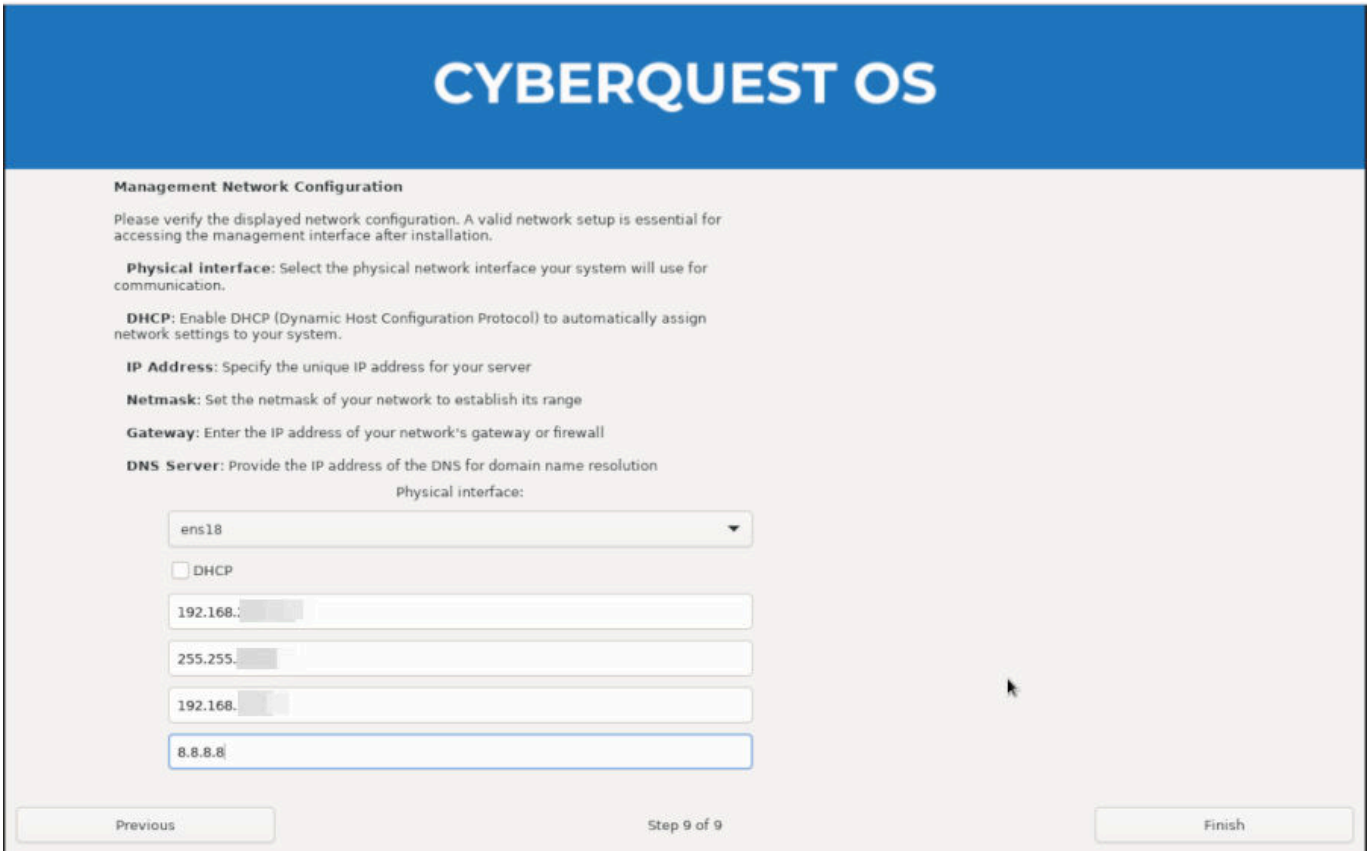


Step 7: Set up the Management Network Configuration using two methods:

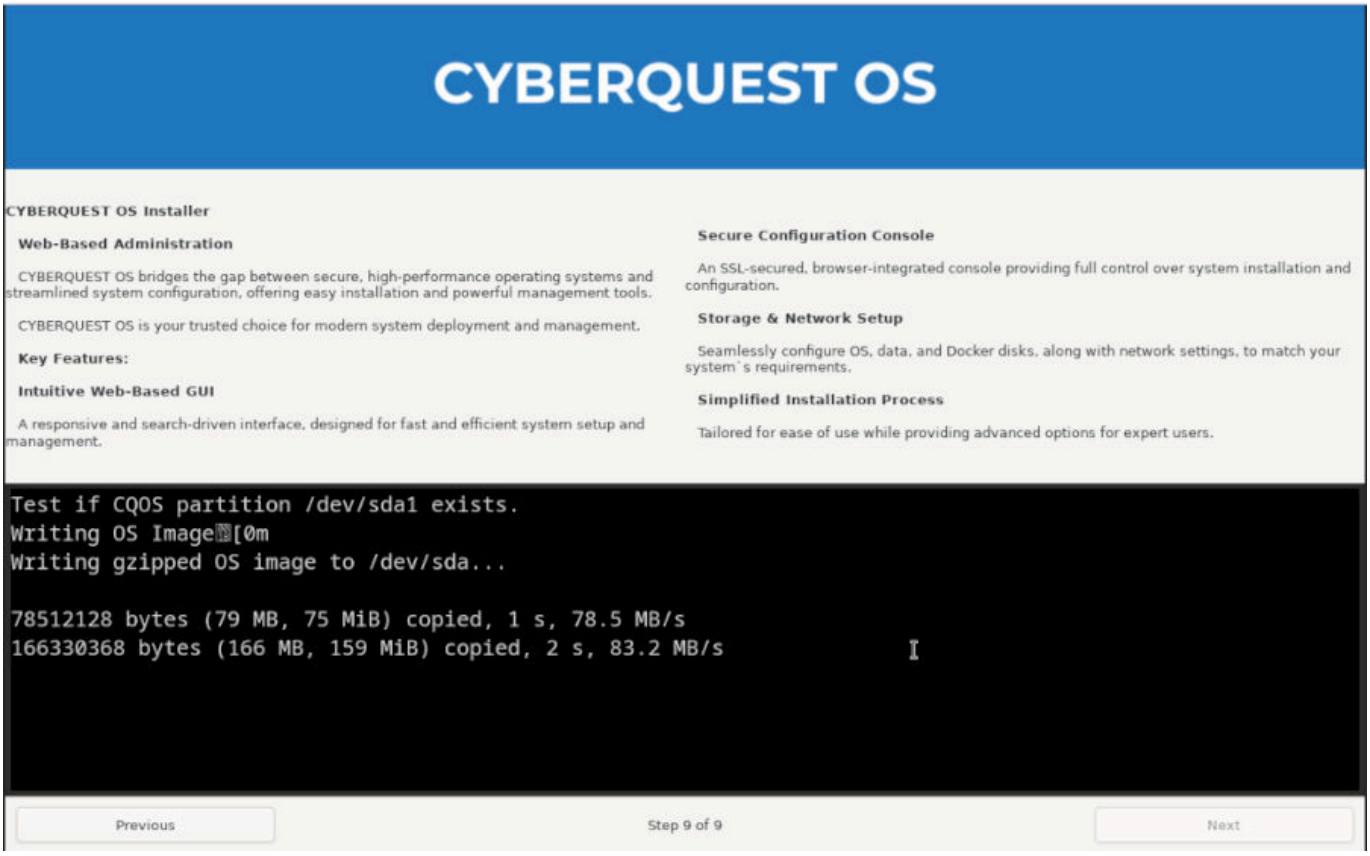
The first method is to use DHCP to automatically assign network settings to the system.

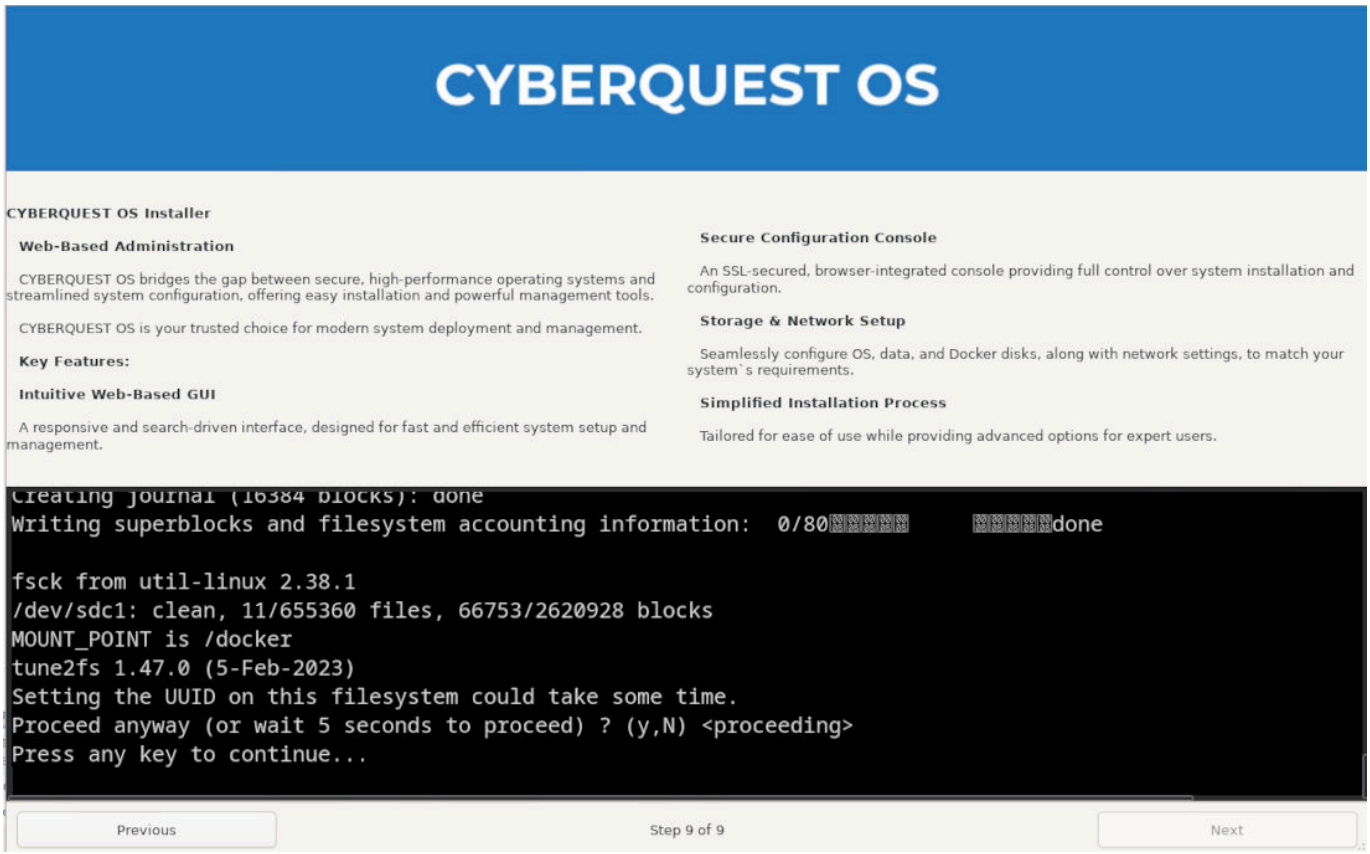


The second method is to manually configure the IP Address, Netmask, Gateway, and DNS Server.

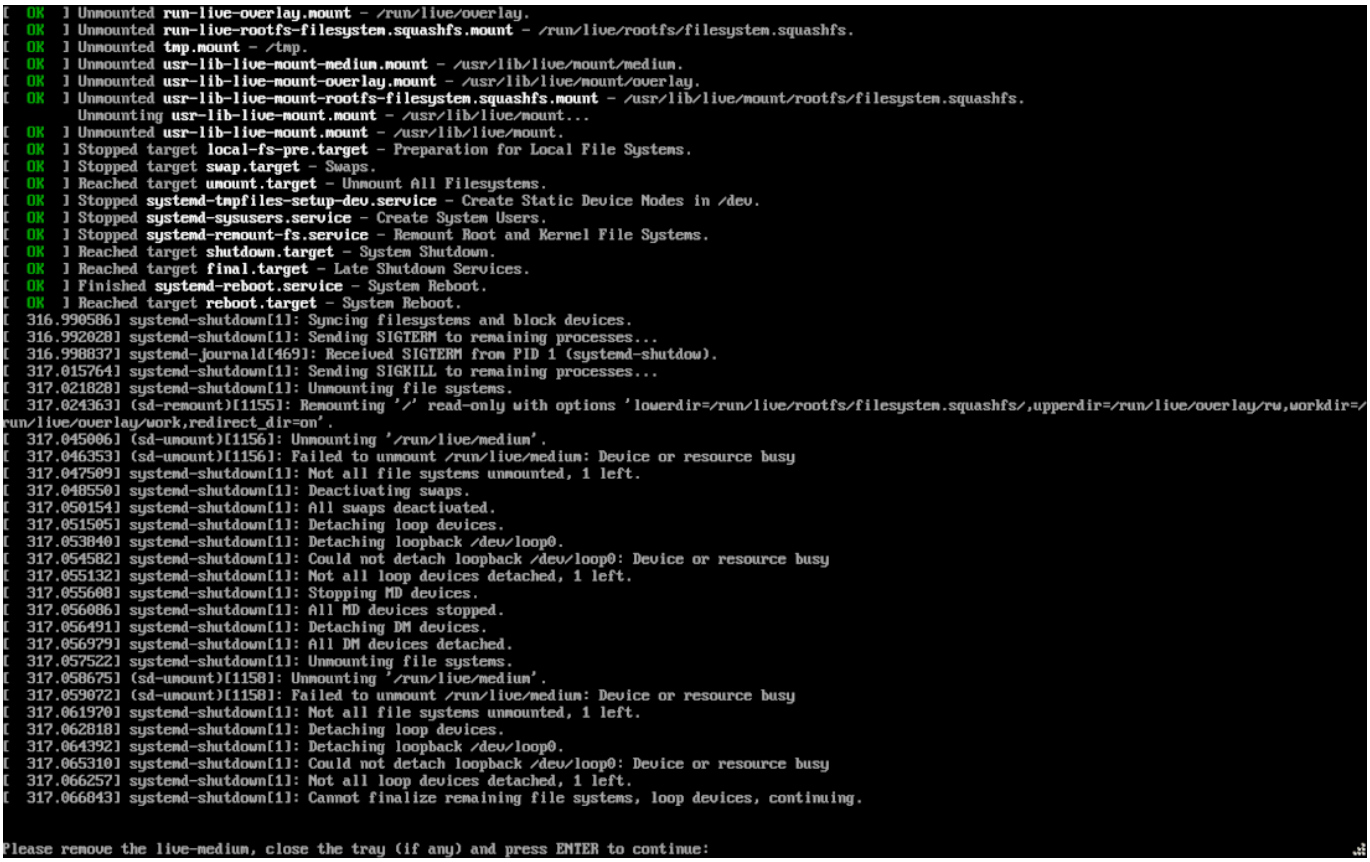


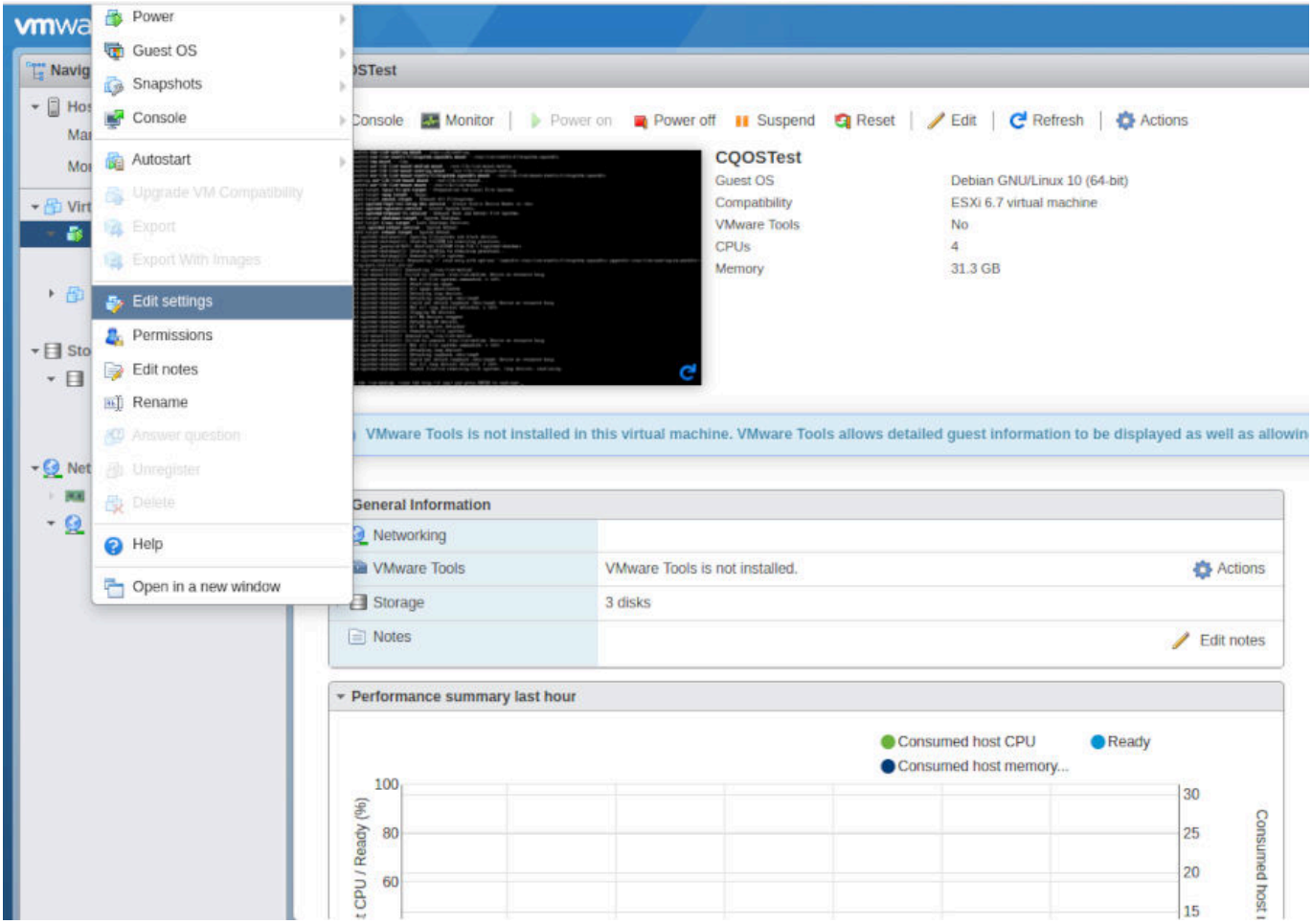
- Click **Finish** and follow the installation prompts. Scroll down to proceed with the installation. Once it's complete, press any key to restart the machine.

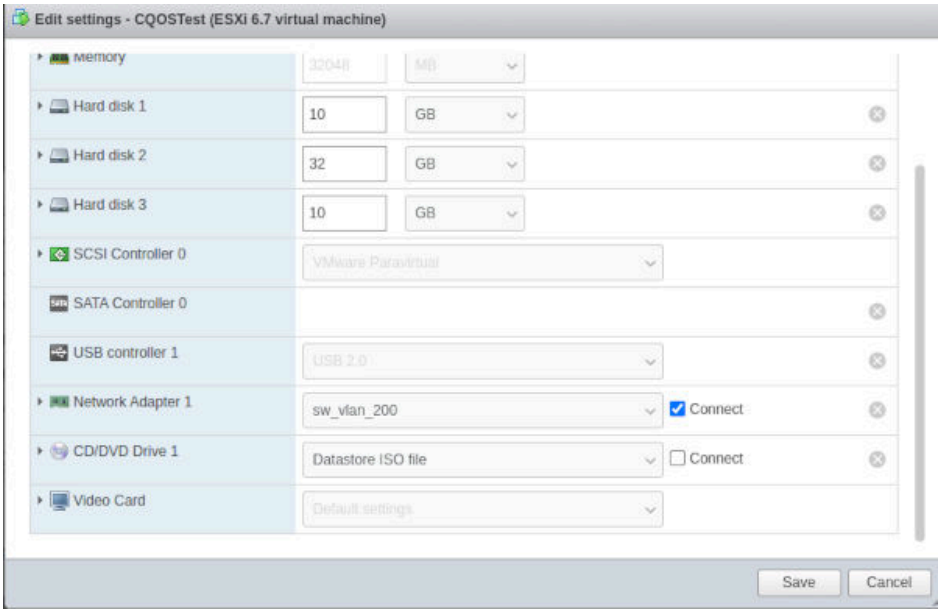


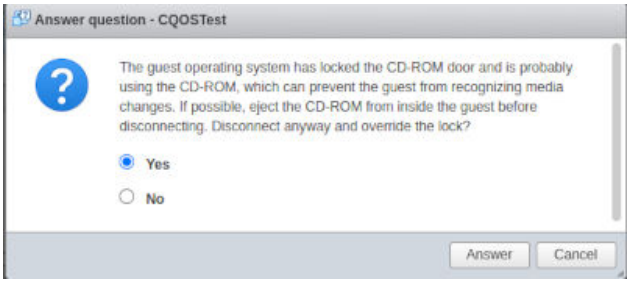


After the restart, the CD will be removed. Right-click on the CQOSTest VM, select **Edit Settings**, then go to **CD/DVD Drive 1**. Deselect **Connect** and click **Save**. After saving, confirm the prompt by selecting **Yes** and press **Answer**.

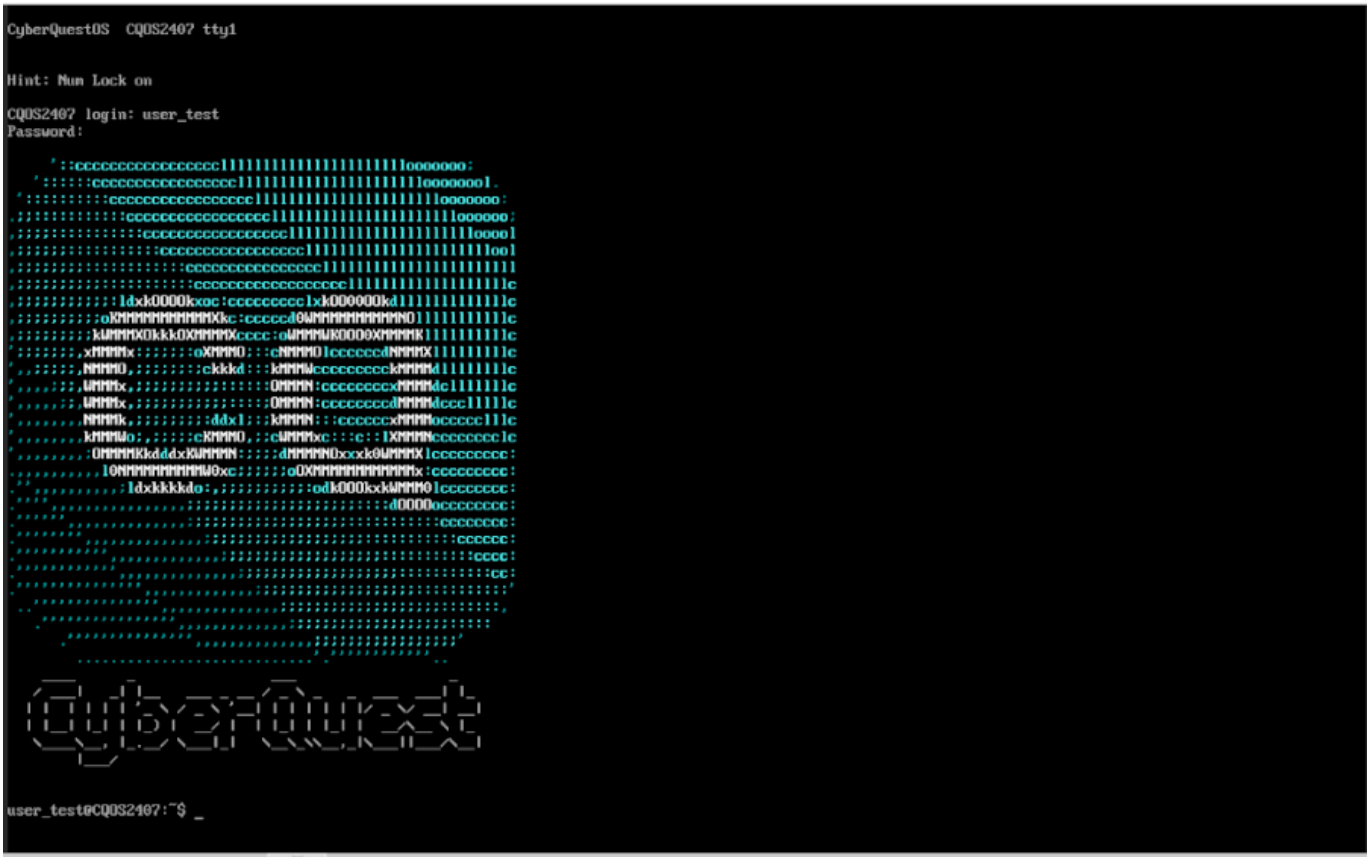








Once the operating system has booted, the user can log in using the credentials created during the installation process above.



CYBERQUEST One-Click Install

The One-Click Install is available for both **Proxmox** and **VMware** installations. It streamlines the installation process by automating the setup of essential components and configurations. ***An internet connection is required to use the One-Click Install***. With just a single command, users can quickly deploy the required environment, reducing setup time and minimizing the potential for configuration errors:

```
mkdir cyberquest-deployment && cd cyberquest-deployment &&  curl -O https://download.cyberquest.cloud/install_for_CQOS_sfx.sh  && sudo bash ./install_for_CQOS_sfx.sh
```

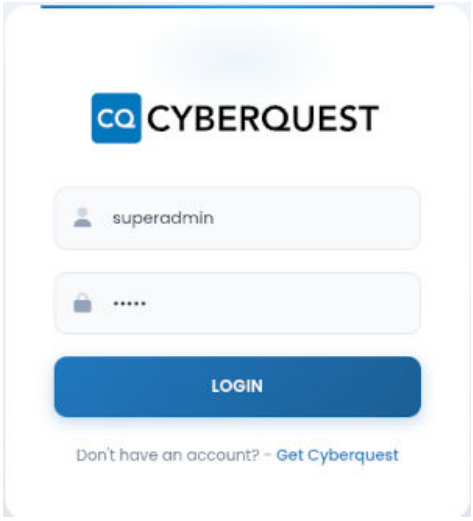
```
docker compose pull
```

```
docker compose up -d
```

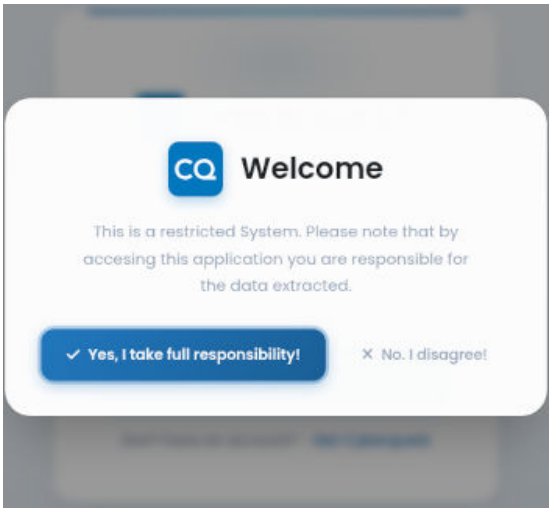
To log in to the CYBERQUEST application, enter the default username and password, then choose the desired interface language.

Default Username: superadmin

Default Password: toor1



You will be prompted with a default message about accessing restricted information. This message is fully customizable.



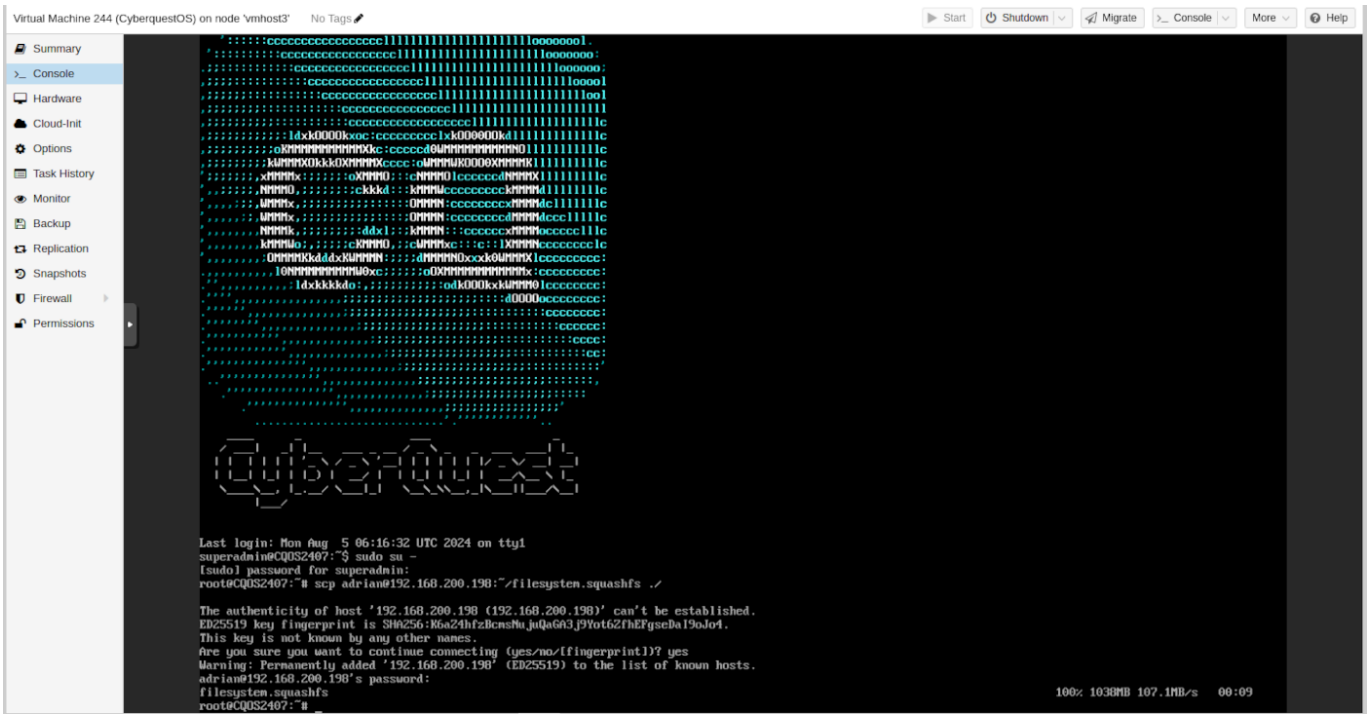
Accept the responsibility by clicking the button "***Yes, I take full responsability!***".Else "***No. I disagree***" and you will be redirected to the authentication page.

OS Upgrade

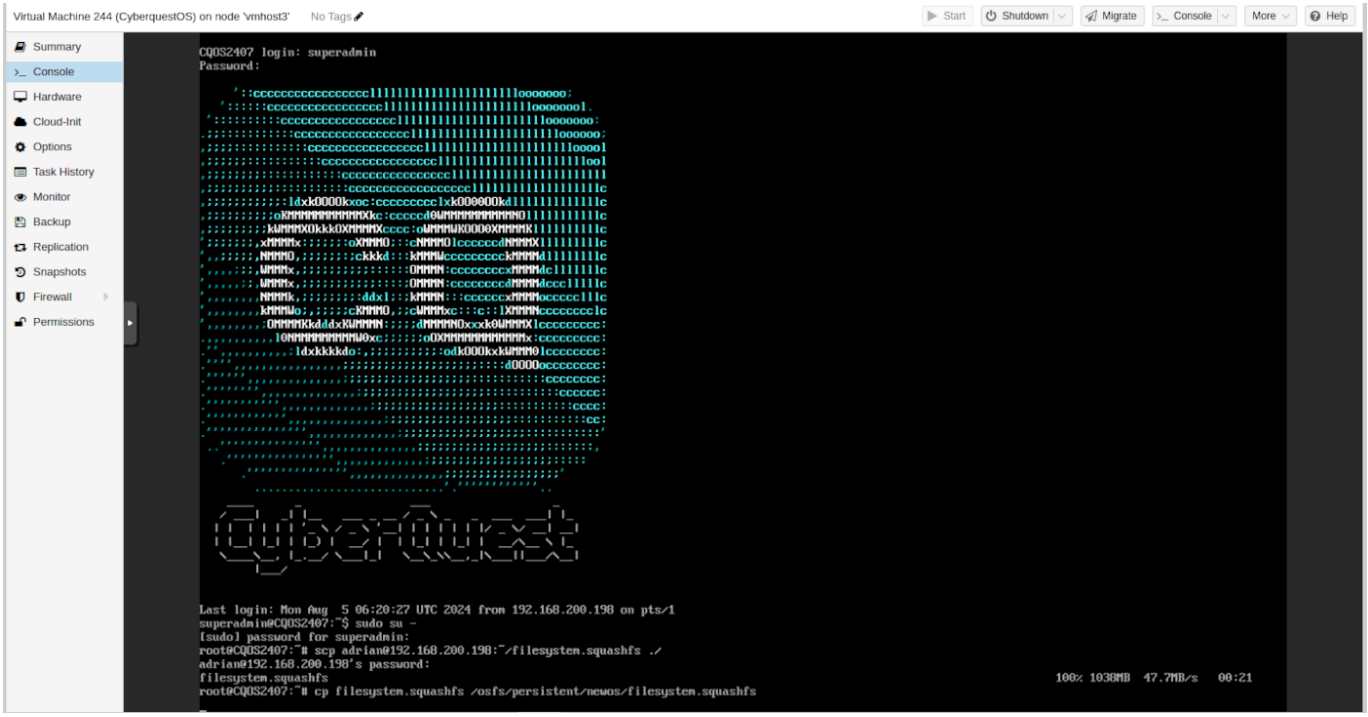
1.Download an Upgrade file from the website www.nextgensoftware.eu (https://www.nextgensoftware.eu).

2.Upload the upgrade file with scp command on the virtual machine CYBERQUEST OS:

```
scp user@computerIP:/path/to/filesystem.squashfs ./
```



3.Copy the file to the folder **/osfs/persistent/newos/**



4.Reboot the CYBERQUEST OS VM

Application Configuration

CYBERQUEST

Copy the package **cyberquest-deployment.tar.gz** in the user's folder and install it as follows:

```
tar -xvf cyberquest-deployment.tar.gz
```

```
cd cyberquest-deployment
```

```
bash keygen.sh
```

```
bash rabbitmq/certRMQ.sh
```

```
bash createDockerVolumes.sh
```

```
docker compose up -d
```

The packet contains the following services:

Services	Description
rabbitmq	Message Queuing
mariadb	Server for storing configurations
redisServer	Memory storage service
data-forward	Module that forwards the events or alerts from CYBERQUEST application to other SIEM's
cerebro	It provides the management interface for the NoSQL service and is only used for troubleshooting
data-correlation	Generate alerts based on real time and correlate events for alerting
data-storage	Long term storage module
data-executor	Execution service
webapplication	Contains the web interface of the solution
data-acquisition	It processes events using API parsers. After the events have been processed, they are sent to: online database (Online DataStorage), Data Storage service and Data Correlation service
data-receiver	A component that **receives data** transmitted over a HTTPS communication
data-server	Is responsible for receiving events and pre-processing them. After this process, the events are sent to the Data Acquisition service using the internal queue service (RabbitMQ)

NETALERT

Copy the **netalert-deployment.tar.gz** package in the user's folder and install it as follows:

```
tar -xvf cyberquest-deployment.tar.gz
```

1.Enter the repository folder

```
cd netalert-deployment
```

2.Setup enviroment

```
echo 'vm.max_map_count=262144' >> /etc/sysctl.conf
echo 'vm.nr_hugepages=5120' >> /etc/sysctl.conf
sysctl -p
```

3.For local docker volume creation (under /data/ folder)

```
bash ./configureVolumes.sh
```

4.Edit docker-compose.yml and set it up:

- data-sense container. example:

```
 ElasticSearchHost=http://127.0.0.1 (add the management ip)
 InterfaceName=enp4s0 (add the zc pf ring interface)
```

- Set-up memory consumed by the Java VM of OpenSearch (default is 8GB).

Example with 3GB:

- Xmx3G (NOT MORE THAN 31 GB and NOT MORE THE 50% of machine RAM)
- we recommend that minimum allocated to be the same as max: Xms3G (minimum allocated)
- opensearch-node container:

```
    "OPENSEARCH_JAVA_OPTS=-Xms3G -Xmx3G"
```

5.Start docker as daemon with command

```
docker compose up -d
```

6.One time only, modify the opensearch container.

- get a shell inside the container

```
 docker exec -it $(docker ps|grep opensearch|cut -d' ' -f1) bash
```

- inside the container execute the following

```
cd plugins/opensearch-security/tools/
```

```
./securityadmin.sh -backup my-backup-directory \
-icl \
-nhnv \
-cacert ../../../config/root-ca.pem \
-cert ../../../config/kirk.pem \
-key ../../../config/kirk-key.pem
```

```
./securityadmin.sh -f ../../../config/opensearch-security/internal_users.yml \
-t internalusers \
-icl \
-nhnv \
-cacert ../../../config/root-ca.pem \
-cert ../../../config/kirk.pem \
-key ../../../config/kirk-key.pem
```

The packet contains the following services:

Services	Description
mldns	In in charge of Machine Learning detections of anomalous DNS traffic (the sample contains the GPU implementation which is suitable JUST for applicances which contains Nvidia GPUs)
mlsmtp	In in charge of Machine Learning detections of anomalous SMTP traffic (the sample contains the GPU implementation which is suitable JUST for applicances which contains Nvidia GPUs)
mltraffic	In in charge of machine learning detections of general network traffic (the sample contains the GPU implementation which is suitable JUST for applicances which contains Nvidia GPUs)
datasense	Performs data-collection from the network card. It needs a supported virtual/physical NIC
apt-scanner	Performs alerting for apt alerts
WebServer	Contains the web interface of the solution
opensearch-node	Contains the opensearch master-node. Additional nodes can be added on the same VM/phisical mashine or other VMs
rabbitmq	Message Queuing
mariadb	Server for storing configurations
syslog-forward	Syslog forwarding components

Development Roadmap

CYBERQUEST Roadmap

CYBERQUEST Development Roadmap

Our commitment to continuous innovation in Security Information and Event Management. This roadmap outlines the features currently in development for CYBERQUEST v2.30 and the strategic direction for the platform's evolution.

Target Version	**v2.30**
Last Updated	March 2026
Expected Delivery	May 2026

Version 2.30 In Development

Target release: May 2026 - Glassmorphism, AI Integration & Regulatory Compliance

`REDESIGN` **Glassmorphism UI/UX Redesign**

Complete visual overhaul of the entire platform with a modern glassmorphism design system. Every page has been redesigned - login, dashboard, browser, alerts, cases, reports, playbooks, entity view, UEBA, vulnerability manager, incidents, anomaly, settings, users/groups, and marketplace. Includes a redesigned navbar and sidebar, premium time interval controls, modern dropdown menus, and comprehensive dark mode support.

`NEW` **OpenSearch Management GUI**

New dedicated interface for OpenSearch/Elasticsearch cluster monitoring and administration with cluster health visualization, index management, and node monitoring.

`NEW` **CyberGlance (System Summary Dashboard)**

New system overview dashboard with chart cards, metrics banner, KPI displays, skeleton loaders, and dark mode support.

`REDESIGN` **Performance Monitoring Redesign**

Complete redesign with instrument-panel metrics and radial ring gauges, expandable detail panel, KPI filtering, and disk I/O throughput monitoring.

`IMPROVED` **AI Personalities**

Renamed from "AI Agents" to "AI Personalities" with structured 3-field prompts (Identity, Instructions, Style), markdown editor, and glassmorphic modal redesign. Added "Generic Data Source Integration Expert" personality.

`NEW` **AI Chatbot (CQ Assistant)**

Fully integrated AI chatbot with sidebar toggle, chat session management, suggestions and commands, personality selector, and multi-provider support (OpenAI-compatible client with Azure OpenAI, LLM ReverseProxy in PHP).

`NEW` **Global Search**

Modern command palette UI (Ctrl+K style) with fuzzy search, result scoring, recent items, Event Type ID search, and expanded navigation items.

`COMPLIANCE` **DORA Compliance Module**

Full DORA incident reporting system with initial notification, intermediate, and final report forms. Includes nomenclature-driven component types, document management, Standard Requirements pages (DORAJourney), Internal Security Documents, and Case Management integration.

`COMPLIANCE` **NIS2 Compliance**

NIS2 incident report support with standard selection in case expand report incident.